



PIERSON FERDINAND

Edmund F. Brown

Founding Partner

4449 Easton Way, Suite 200

Columbus, Ohio 43219

Direct: 614.245.8418

Fax: 866.414.5083

Email: Edmund.brown@pierferd.com

www.pierferd.com

March 12, 2025

VIA EMAIL DELIVERY (Idtheft@oag.state.md.us)

Office of the Attorney General

Attn.: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Notice of Data Breach

Dear Sir or Madam:

This firm represents Fall Mountain Regional School District ("Fall Mountain RSD") in connection with the above-referenced matter. Please accept the following as formal *Security Breach Notification* with respect to a security incident involving Fall Mountain RSD's information.

On November 5, 2024, certain sensitive information was inadvertently disclosed to an unauthorized third party via email. Fall Mountain RSD takes the security of sensitive information in its possession very seriously. Upon discovery, Fall Mountain RSD launched an internal investigation into this incident to identify the full extent of data potentially exposed as a result of this incident. Based on a thorough investigation of the data, it was determined that information related individuals' first name, last name and Social Security number were subject to unauthorized access. At this time, Fall Mountain RSD is not aware of any misuse of this information.

Fall Mountain RSD has made immediate enhancements to its systems, security and practices. Additionally, they have engaged appropriate experts to assist in conducting a full review of its security practices and systems to ensure that enhanced security protocols are in place going forward. Fall Mountain RSD is committed to helping those people who may have been impacted by this unfortunate situation. Fall Mountain RSD has secured the services of Experian to provide identity theft protection and credit monitoring services to the affected individuals for 12 months at no cost. Based on findings from the investigation, Fall Mountain RSD has determined that certain personal information belonging to one (1) Maryland resident was contained in affected email account.

Fall Mountain RSD provided direct notice to the impacted Maryland resident on or about March 3, 2025. A draft of the notification letter sent to the Maryland resident is attached as Exhibit A. The notification outlines the nature of the incident, the steps that Fall Mountain RSD took to remediate the incident and offers complimentary identify theft



PIERSON FERDINAND

Office of the Attorney General
Attn.: Security Breach Notification
March 12, 2025
Page 2 of 2

protection and credit monitoring services to the affected individual. The letter also contains specific instructions for enrolling in the free services previously described.

Should you have any questions or concerns, please contact me directly at (614) 245-8418 or at edmund.brown@pierferd.com.

Very truly yours,

Edmund F. Brown



EXHIBIT A

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

RE: Important Security Notification. Please read this entire letter.

Dear <<Full Name>>:

Fall Mountain Regional School District (“Fall Mountain”) recently discovered an incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What Happened? On November 5, 2024, certain sensitive information was inadvertently disclosed to an unauthorized third party. Fall Mountain takes the security of sensitive information in its possession very seriously. Upon discovery, we launched an internal investigation into this incident to identify the full extent of data potentially exposed as a result of this incident.

What Information Was Involved? Based on a thorough investigation of the data, it was determined that information related individuals’ first name, last name and Social Security number were subject to unauthorized access. At this time, we are not aware of any misuse of this information.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Fall Mountain has made immediate enhancements to our systems, security and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation.

BEGIN EXPERIAN REQUIRED PRODUCT LANGUAGE

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<CM Duration>> months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for <<CM Duration>> months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary <<CM Duration>>-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: <<Activation Code>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by <<Enrollment Deadline>>. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<CM Duration>>-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont 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 reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. 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 5 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. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission 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 immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call 888-802-9344 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time.

Sincerely,



Debra Livingston Manseau
Superintendent
Fall Mountain Regional School District

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.