MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 19, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rockwood School District, ("RSD"), located at 111 East North Street, Eureka, MO, 63025 and are writing to notify your Office of an incident that may affect the security of some personal information relating to seven (7) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, RSD does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about June 17, 2021, RSD discovered that certain computer systems in its network had been infected with malware which prevented access to certain files on those systems. Upon discovery, RSD immediately notified law enforcement and began an investigation with the assistance of third-party computer forensic specialists. Through this investigation, it was determined that RSD was the victim of a criminal ransomware attack. Furthermore, the investigation recently determined that certain RSD systems were subject to unauthorized access on separate occasions between April 20, 2021 and June 24, 2021. While the investigation was able to determine that certain RSD systems were accessed, the investigation was unable to confirm what information within those systems was actually accessed. Therefore, out of an abundance of caution, RSD conducted an extensive review of the contents of the impacted systems in order to provide notice to impacted individuals.

The information related to New Hampshire residents that could have been subject to unauthorized access varied by individual but includes name, address, Missouri student identification number, student record information, Social Security number, and/or financial account information.

Notice to New Hampshire Residents

On or about August 19, 2021, RSD began providing written notice of this incident to affected individuals, which includes approximately seven (7) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. RSD also posted notice of this incident on its website. A copy of RSD's website notice is attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

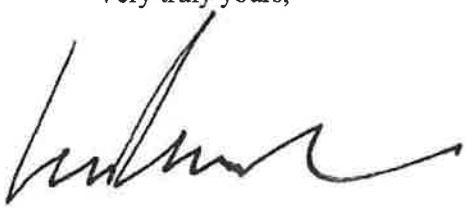
Upon discovering the event, RSD moved quickly to investigate and respond to the incident, assess the security of RSD systems, and notify potentially affected individuals. RSD is also working to implement additional safeguards and training to its employees. RSD is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

Additionally, RSD is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or event, or wish to discuss this matter further, please contact us at 267-930-4637.

Very truly yours,



Gregory Lederman of
MULLEN COUGHLIN LLC

Enclousre
GCL/mwj

EXHIBIT A

ROCKWOOD SCHOOL DISTRICT

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

The Rockwood School District ("District") is writing to inform you of a recent incident which may impact some of your information. The confidentiality, privacy and security of information in the District's care is one of its highest priorities and the District takes this incident very seriously. We are providing you with information about the event, our response, and steps you may take to better protect your information, should you feel it is appropriate to do so.

What Happened? On June 17, 2021, the District discovered that certain computer systems in its network had been infected with malware which prevented access to certain files on those systems. Upon discovery, the District immediately notified law enforcement and began an investigation with the assistance of third-party computer forensic specialists. Our investigation recently determined that certain RSD systems were subject to unauthorized access between April 20, 2021 and June 24, 2021. Through this investigation, it was determined that the District was the victim of a criminal ransomware attack. While the investigation was able to determine that certain District systems were accessed, the investigation was unable to confirm what information within those systems was actually accessed. Therefore, out of an abundance of caution, we conducted an extensive review of the contents of the impacted systems in order to provide notice to impacted individuals.

What information was involved? Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because certain information related to you may have been on the impacted systems. The impacted information relating to you includes: <<b2b_text_1(DataElements)>>.

What Are We Doing? Rockwood School District takes the confidentiality and security of information very seriously. We promptly investigated this incident and took steps to secure our systems. We also implemented additional security measures and we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. As an added precaution, we are providing you with access to complimentary identity monitoring services through Kroll for one year.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. We also encourage you to review the "*Steps You Can Take to Help Protect Your Information*" section of this letter.

For More Information. If you have additional questions, please call 1-XXX-XXX-XXXX, Monday through Friday from 8:00 a.m. – 5:30 p.m. Central Time (excluding some U.S. holidays). Additional information, including frequently asked questions, can be found on the District's website at rsdmo.org.

Please know that we share your concern and regret the inconvenience and anxiety this situation has caused for everyone involved. Rockwood School District remains committed to protecting the information in our care and will continue to take steps to continuously improve and enhance the security of our systems.

Sincerely,

Deborah Ketring

Deb Ketring
Chief Information Officer
The Rockwood School District

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **November 17, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

Additional information describing your services is included with this letter.

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

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington,

DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are # Rhode Island residents impacted by this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

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 will be able to help you determine if it is an indicator of identity theft.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.

EXHIBIT B

NOTICE OF DATA PRIVACY INCIDENT

Rockwood School District (the "District") is providing notice of a recent incident that may affect the security of information pertaining to individuals, including certain current and former students and employees. The confidentiality, privacy, and security of information in the District's care is one of its highest priorities and the District takes this incident very seriously. Although the District has not received any reports of actual or attempted misuse of the impacted information, the District is providing this notice in an abundance of caution.

What Happened? On June 17, 2021, the District discovered that certain computer systems in its network had been infected with malware which prevented access to certain files on those systems. Upon discovery, the District immediately notified law enforcement and began an investigation with the assistance of third-party computer forensic specialists. The investigation recently determined that certain District systems were subject to unauthorized access between April 20, 2021 and June 24, 2021. Through this investigation, it was determined that the District was the victim of a criminal ransomware attack. While the investigation was able to determine that certain District systems were accessed, the investigation was unable to confirm what information within those systems was actually accessed. Therefore, out of an abundance of caution, the District conducted an extensive review of the contents of the impacted systems in order to provide notice to impacted individuals.

What information was involved? The information contained within the files at issue varied by individual but contained names, addresses, Social Security numbers, dates of birth, financial account information, District employee identification numbers, MOSIS identification numbers, and/or student records. The District does not have any evidence that information was subject to actual or attempted misuse as a result of this incident.

What Are We Doing? The District takes the confidentiality and security of information very seriously. The District promptly investigated this incident and took steps to secure its systems. The District also implemented additional security measures and is reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. The District is also offering credit monitoring for individuals whose information was impacted.

For more information. We understand some people may have additional questions concerning this incident. Individuals can direct questions to (636) 733-1111 Monday –Friday between 7:00 a.m. and 4:30.

What Can You Do? The District encourages you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. The District apologizes for any inconvenience this may cause and remains committed to the privacy and security of all information it maintains.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which

is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.