EXHIBIT 1

Uintah School District ("Uintah") writes to notify your office of a data privacy event. Uintah is located at 826 South 1500 East, Naples, UT 84078. By providing this notice, Uintah does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 9, 2025, Uintah identified suspicious activity on its computer network. Uintah promptly launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that there was unauthorized access to the Uintah network on April 9, 2025, and that, during that period of unauthorized access, certain information stored within the Uintah network was accessed and/or copied without permission. Uintah then undertook a comprehensive and time-intensive review of the involved files to determine what types of information were impacted, to whom that information related, and to identify contact information for purposes of providing notifications. That process recently completed, at which point Uintah provided notice to individuals whose information was contained within the impacted files.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Nebraska Residents

On or about August 7, 2025, Uintah provided written notice of this incident to approximately two (2) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Uintah moved quickly to investigate and respond to the same, assess the security of Uintah systems, and identify potentially affected individuals. Uintah is also working to implement additional safeguards and training to its employees. Uintah also provided one (1) year of complimentary credit monitoring to all employees when Uintah first identified this event in April 2025. Uintah is also providing access to credit monitoring services for one (1) year through TransUnion to any individuals whose personal information was potentially affected by this incident and who resides in a state where provision of complimentary credit monitoring is required, to the extent that those are not employees who previously received an offer of monitoring in April.

Additionally, Uintah is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Uintah is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

Uintah is also providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Uintah School District

000010102G0400 P

August 7, 2025

NOTICE OF SECURITY INCIDENT

Dear

Uintah School District ("Uintah") writes to inform you of a recent event that may have impacted the confidentiality of some of your information. Although we are unaware of any identity theft or fraud occurring as a result of this event, we are providing you with information about the event, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On April 9, 2025, Uintah identified suspicious activity on our computer network. We promptly launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that there was unauthorized access to our network on April 9, 2025 and that, during that period of unauthorized access, certain information stored within our network was accessed and/or copied without permission. We therefore undertook a comprehensive and time-intensive review of the involved files to determine what types of information were impacted, to whom that information related, and to identify contact information for purposes of providing notifications. That process was recently completed, and we are providing you with notification given that your information was contained within the impacted files.

What Information Was Involved? Our investigation and review determined that the following types of information related to you were found in the impacted files: your name, Social Security number. At this time, we have no evidence that your information was used to commit identity theft or fraud as a result of this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon becoming aware of the referenced suspicious activity, we promptly commenced an investigation to confirm the nature and scope of the event. We are also reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar events moving forward. We are also notifying impacted individuals, including you, so you may take steps to better protect your information, should you feel it is appropriate to do so.

As an added precaution, we are also offering you 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 twelve 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 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. Individuals who wish to receive these services must enroll by following the below enrollment instructions, as we are unable to activate them on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors. Additional information and resources are included in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also enroll in the complementary credit-monitoring services available to you.

For More Information. If you have additional questions, representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, at 1-833-397-7015 from Mondays through Fridays between 8:00am to 8:00pm Eastern time, excluding holidays. You may also write to Uintah at 826 South 1500 East, Naples, UT 84078.

Sincerely,

Uintah School District

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: 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.

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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

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 Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 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.