EXHIBIT 1

By providing this notice, Uinta Bank ("UB") 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 or about December 19, 2025, UB became aware of a suspicious activity related to its computer environment. UB immediately implemented its incident response plan to limit the scope of the event. UB worked with third-party specialists to investigate what occurred and to restore UB's systems. The disruption to operations was minimal, and all UB operations were fully restored. The investigation confirmed that an unauthorized actor gained access to certain UB systems on December 19, 2025, and copied some files without permission. UB then underwent a thorough review of the files that were copied without permission to determine whether any sensitive information was contained therein and to whom the information relates. On April 21, 2026, this review was completed, and UB worked quickly to confirm address information for the individuals that may have been impacted. Please note, it has been confirmed that the unauthorized actor does not have the ability to access customer bank accounts.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number, and financial account information.

Notice to Nebraska Residents

On or about May 7, 2026, UB provided written notice of this incident to twenty-two (22) 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 discovering the event, UB moved quickly to implement its incident response plan, investigate the incident, assess the security of UB systems, and identify potentially affected individuals. Further, UB notified federal law enforcement and its primary federal regulator regarding the event. UB is also reviewing its policies, procedures, and safeguards in place in order to limit the likelihood of a similar event. UB is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, UB is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. UB 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.

UB is 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

Uinta Bank
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

Uinta Bank

7795

May 7, 2026

NOTICE OF SECURITY INCIDENT

Dear :

Uinta Bank ("UB") is writing to let you know about an incident that involves some of your personal information. This letter provides an overview of the incident, our response, and steps you may take to better protect your information, should you feel it appropriate to do so.

What Happened? On December 19, 2025, UB became aware of suspicious activity related to its computer environment. UB immediately implemented its incident response plan to limit the scope of the incident. UB worked with third-party specialists to investigate what occurred and to restore UB's systems. The disruption to operations was minimal, and all UB operations were fully restored. The investigation confirmed that an unauthorized actor gained access to certain UB systems on December 19, 2025, and copied some files without permission. UB then underwent a thorough review of the files that were copied without permission to determine whether any sensitive information was contained therein and to whom the information relates. On April 21, 2026, this review was completed, and UB worked quickly to confirm address information for the individuals that may have been impacted. Please note, it has been confirmed that the unauthorized actor does not have the ability to access customer bank accounts.

What Information Was Involved? The information that was in the impacted files includes your name and Social Security number and financial account information.

What We Are Doing. We take the confidentiality and privacy of the information in our care very seriously. Upon learning of the incident, UB took immediate steps to secure our network and limit the scope of the incident. Due to the prompt implementation of our incident response plan, UB was able to restore its systems quickly with limited operational impact. Additionally, UB promptly notified law enforcement and its primary federal regulator. We are reviewing our policies, procedures, and safeguards in place in order to limit the likelihood of a similar event.

Although we do not have any indication of identity theft, fraud, or impact to any customer bank accounts resulting from this incident, as an added precaution, UB is providing you with complimentary access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for 12 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. Please note that you will need to enroll yourself in these services, as we are not able to do so on your behalf due to privacy restrictions. You can find instructions regarding how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Personal Information* that contains guidance regarding what you can do to better protect your information and information on how to enroll in the complimentary credit monitoring services we are making available to you. Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 1-833-289-2068, Monday through Friday, from 8:00 am to 8:00 pm Eastern Time, excluding major U.S. holidays. You may also write to UB at 301 2nd Street, Rock Springs, WY 82901.

Sincerely,

Uinta Bank

Steps You Can Take To Help Protect Personal 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 1 Rhode Island residents that may be impacted by this event.