

EXHIBIT 1

By providing this notice, Sodoro Law Group, LLC (“SLG”) 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 September 16, 2025, SLG became aware of suspicious activity within its email tenant. SLG confirmed containment of the email environment and initiated an investigation with the assistance of outside professionals. The investigation determined that an unauthorized third party accessed a SLG employee email account between September 15, 2025, and September 16, 2025, and acquired information contained within certain emails. A diligent review and validation of emails involved was conducted to identify whether they contained personal information, and if so, what personal information they contained and to whom that information relates. This process, which completed on January 19, 2026, identified that the affected emails contained certain personal information.

The personal information involved includes name, driver’s license or state identification number, Social Security number, and username and password.

Notice to Nebraska Residents

On or about February 13, 2026, SLG began providing written notice of this event to approximately twelve (12) 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, SLG contained its email environment, conducted an investigation as described above, and is notifying individuals whose personal information was identified in the emails involved in the event. SLG is reviewing its existing policies and procedures to help reduce the likelihood of a similar event occurring in the future. SLG is providing access to credit monitoring services for twelve (12) months, through Cyberscout, a TransUnion company, to individuals whose personal information was present in the emails involved, at no cost to these individuals.

Additionally, SLG is providing notified 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. SLG 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.

EXHIBIT A



Sodoro Law Group, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2978



February 18, 2026

Dear [REDACTED]:

Sodoro Law Group, LLC (“SLG”) is writing to inform you of an event that involves your personal information. This letter provides you with information about what happened, our response, and steps you can take to help protect your personal information, should you feel it appropriate to do so.

What Happened? On September 16, 2025, we became aware of suspicious activity within our email tenant. We confirmed containment of our email environment and initiated an investigation with the assistance of outside professionals. The investigation determined that an unauthorized third party accessed a SLG employee email account between September 15, 2025, and September 16, 2025, and acquired information contained within certain emails. A diligent review and validation of emails involved was conducted to identify whether they contained personal information, and if so, what personal information they contained and to whom that information relates. This process, which completed on January 19, 2026, identified that the affected emails contained some of your personal information.

What Information Was Involved? The personal information present in the emails involved includes your name and the following: [REDACTED]

What We Are Doing. Upon learning of this event, we contained the email environment, conducted an investigation as described above, and are notifying individuals whose personal information was identified in the emails involved in the event. We are reviewing our existing policies and procedures to help reduce the likelihood of a similar event occurring in the future.

In addition, we are 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 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. More information about the services and how to enroll in them is provided in the enclosed *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant in protecting against identity theft and fraud, including by reviewing your account statements and monitoring your credit reports for suspicious activity. Suspicious activity should be reported promptly to your credit card company and/or bank.

Information about how to obtain a free credit report, credit freeze, and other guidance is provided in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. If you have questions, please call our assistance line at 1-800-405-6108 8:00 a.m. to 8:00 p.m. Eastern time, excluding holidays. You can also write to SLG at 13924 Gold Circle, Omaha, Nebraska 68144.

Sincerely,

Sodoro Law Group



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: [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.

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.