

EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SSEK 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 March 5, 2025, SSEK became aware of potential access to data within its network. SSEK promptly responded and launched an investigation to confirm the nature and scope of the incident. Through the investigation, SSEK learned that an unauthorized actor copied certain data without permission. SSEK then conducted a time intensive and thorough review of the data that was at risk to determine what was contained therein and to whom it relates for purposes of providing notice. This review was recently completed, and SSEK is notifying affected individuals.

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

Notice to Nebraska Residents

On or about June 20, 2025, SSEK will provide written notice of this incident to 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 discovering the event, SSEK moved quickly to investigate and respond to the incident, assess the security of SSEK systems, and identify potentially affected individuals. SSEK is also working to implement additional safeguards and training to its employees. SSEK 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, SSEK is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SSEK is providing individuals with information on how to place a fraud alert and security freeze on their 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.

SSEK is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A



Shepherd Smith Edwards & Kantas, LLP
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1197



June 20, 2025

NOTICE [Redacted]

Dear [Redacted]

Shepherd Smith Edwards & Kantas, LLP (“SSEK”) writes to notify you of an incident that may impact the privacy of some of your information. While we have no evidence of misuse of information as a result of this incident, out of an abundance of caution, we are providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On March 5, 2025, SSEK became aware of potential access to data within our network. We promptly responded and launched an investigation to confirm the nature and scope of the incident. Through the investigation, we learned that an unauthorized actor copied certain data without permission. We then conducted a time intensive and thorough review of the data that was at risk to determine what was contained therein and to whom it relates for purposes of providing notice. This review was recently completed and we are notifying you because certain information of yours was contained in the files.

What Information Was Involved? The information that was present in the files viewed or accessed as a result of this incident could include your name, [Redacted]
[Redacted] At this time, we have no indication that your information was misused or used to commit identity theft or fraud as a result of this incident.

What Are We Doing? The confidentiality, privacy, and security of personal information is among SSEK’s highest priorities, and we have security measures in place to protect information in our care. Upon discovery, we notified law enforcement and promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying potentially impacted individuals. While we have measures in place to protect information in our care, as part of our ongoing commitment to the privacy of information, we continue to review our policies, procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities where necessary.

As an added precaution, we are providing you with twelve months of complimentary access to credit monitoring and identity restoration services through Transunion, at no cost to you. Should you wish to receive these services, you will need to enroll yourself as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Your Personal Information*.

What You Can Do. 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. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call 1-800-405-6108 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Individuals may also write to SSEK at 1010 Lamar St #900, Houston, TX 77002. We take this incident seriously and sincerely regret any inconvenience or concern this incident may have caused you.

Sincerely,

Shepherd Smith Edwards & Kantas, LLP

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring Services

In response to the incident, we are providing you with 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 [REDACTED] 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.

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 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 Ave 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 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 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.