EXHIBIT 1

By providing this notice, The Society of Certified Insurance Counselors Inc. dba Risk & Insurance Education Alliance ("SCIC") 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 June 16, 2025, SCIC became aware of suspicious activity related to a company email account. Upon learning of this activity, SCIC disabled the account, took steps to secure its email environment, and launched an investigation with the assistance of third-party cybersecurity specialists. This investigation determined that between June 15, 2025 and June 16, 2025, an unauthorized actor gained access to a company email account, which allowed them to download files from SharePoint. SCIC therefore conducted a thorough review of the files believed to be downloaded by the unauthorized actor, in order to identify individuals whose information was potentially accessed during the period of compromise. That review was recently completed.

The information impacted for residents of your state includes name and Social Security number.

Notice to Nebraska Residents

On or about November 20, 2025, SCIC provided written notice of this incident to approximately four (4) 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, SCIC moved quickly to investigate and respond to the incident, assess the security of SCIC systems, and identify potentially affected individuals. SCIC is also working to implement additional safeguards. SCIC is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SCIC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SCIC is providing individuals with 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.

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

EXHIBIT A

The Society of Certified
Insurance Counselors Inc.

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: February 20, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 20, 2025

NOTICE OF <<Variable Header: SECURITY INCIDENT /DATA BREACH>>

Dear <<First Name>> <<Last Name>>:

The Society of Certified Insurance Counselors Inc. dba Risk & Insurance Education Alliance ("SCIC") writes to inform you of an event that may affect the privacy of some of your information. Although we are unaware of any identity theft or fraud in relation to the event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On June 16, 2025, SCIC became aware of suspicious activity related to a company email account. Upon learning of this activity, we disabled the account, took steps to secure our email environment, and launched an investigation with the assistance of third-party cybersecurity specialists. This investigation determined that between June 15, 2025 and June 16, 2025, an unauthorized actor gained access to a company email account, which allowed them to download files from SharePoint. We therefore conducted a thorough review of the files believed to be downloaded by the unauthorized actor, in order to identify individuals whose information was potentially accessed during the period of compromise. That review recently completed.

What Information Was Involved? Through our review, we determined that the following types of information were stored within the impacted account at the time of the event: your name and Social Security number. Again, SCIC is not aware of any actual or attempted identity theft or fraud in relation to this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon learning of this event, we took steps to secure our email environment and 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. Additionally, we are notifying potentially impacted individuals, including you, so they may take steps to best protect their information, should they feel it is appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<Membership Offering Length: twelve (12)/twenty-four (24)>> months at no cost to you, through IDX. You can find information on how to enroll in these services in the enclosed *Steps You Can Take to Protect Your Personal Information.* We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements as well as monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. Please also review the information contained in the enclosed *Steps You Can Take to Protect Your Personal Information*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 1-833-788-9712 from 9 am – 9 pm Eastern Time, Monday through Friday, excluding major U.S. holidays. We take the privacy and security of personal information in our care very seriously and sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

The Society of Certified Insurance Counselors

Steps You Can Take To Protect Your Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is February 20, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

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 oag.maryland.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 is approximately 1 Rhode Island resident that may be impacted by this event.