

EXHIBIT 1

By providing this notice, the Institute 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

The Institute became aware of suspicious activity and promptly began an investigation into the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to certain Institute systems and copied files from those system on or around May 5, 2025. The Institute then undertook a review of the relevant files in order to determine what data was present and to whom it related. On or about August 26, 2025, the Institute completed its review. Thereafter, the Institute worked to reconcile the records and confirm address information in order to provide notification to potentially affected individuals. Based on these efforts, on October 1, 2025, it was determined that notice would be provided to ten (10) Nebraska residents. The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Nebraska Residents

On September 26, 2025, the Institute notified individuals via a posting on its website and notice to the media in all fifty states. On or about October 6, 2025, the Institute provided written notice of this incident to ten (10) 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

In response to this incident, the Institute promptly took steps to assess the security of its systems and initiated a thorough forensic investigation. The Institute also promptly notified the Department of Education. Additionally, the Institute is working to enhance its technical safeguards and will continue to evaluate and evolve its cybersecurity posture.

The Institute is also providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. The Institute is also providing those individuals whose Social Security number may be affected access to credit monitoring services for one (1) year, through Epiq. The Institute is also providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A



Institute of
Culinary Education
EST. 1975
NEW YORK | LOS ANGELES | ONLINE



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

<<VAR DATA 1/CA HEADER>>

Dear <<Full Name>>:

The Institute of Culinary Education (the “Institute”) is writing to make you aware of an event that may affect some of your information. Although the Institute has no indication that any identity theft or fraud occurred as a result of this event, this notice provides information about this event, our response, and resources available to you to help protect your information, should feel it is appropriate.

What Happened? The Institute became aware of suspicious activity and promptly began an investigation into the nature and scope of the activity. Our investigation determined that an unauthorized actor gained access to certain Institute systems and copied files from those systems on or around May 5, 2025. We undertook a review of the relevant files in order to determine what data was present and to whom it related. We recently determined <<Var Data 2/WA and RI Text>> that information related to you was present in the relevant files. We then worked to reconcile the records and confirm contact information in order to provide you with this notice.

What Information Was Involved? Our review determined that information present in the relevant files included your <<Data Elements>>, and name.

What We Are Doing. We take the security of information in our care very seriously. Upon becoming aware of the issue, we promptly launched an investigation into the nature and scope of the event and took measures to ensure the security of our environment. Additionally, we have also implemented additional cybersecurity measures. As an added precaution, we are offering you access to credit monitoring and identity theft protection services for <<12/24>> months at no cost to you, through Epiq. We encourage you to enroll in these services as we are unable 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 and credit reports for suspicious activity and to detect errors. In addition, you can enroll in the free credit monitoring services that we are providing. Please note, you must enroll by <<Enrollment Deadline>> to take advantage of these services. We also recommend you review the *Steps You Can Take to Help Protect Your Information* section of this letter to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it is appropriate to do so. In this section, you will also find enrollment instructions for credit monitoring services.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions or need assistance, please call 855-291-2584 between the hours of Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern, except US holidays. You may also write to us at 225 Liberty Street, New York, NY 10281.

Sincerely,

The Institute of Culinary Education

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

- 1) Visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<**Activation Code**>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Privacy Solutions ID provides credit monitoring through Equifax, credit report and score access, \$1 million identity theft insurance with \$0 deductible, ID Restoration services, and dark web monitoring. See below for more details.

Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

1-Bureau Credit Score and Report

Annual 1-Bureau VantageScore and 1-Bureau Credit Report

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, and payment platform, with alerts.

Dark Web Monitoring

Searches for compromised information across the dark web, with alerts.

Credit Report Lock/Freeze

Assists with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Lost Wallet Assistance

Assistance with canceling and reissuing credit and ID cards.

Identity Restoration

Dedicated ID restoration specialists who assist with ID theft recovery.

Up to \$1M Identity Theft Insurance

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity--occurrence based.

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID, please call directly at 866-675-2006, Monday-Friday 9:00 a.m. to 5:30 p.m., EST.

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/](http://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 <<RI Count>> Rhode Island residents that may be impacted by this event.