

July 31, 2026

Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

VIA PORTAL ONLINE

Re: Notification of Data Security Event

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Sullivan Environmental Services, Inc. ("SES") located at PO Box 17017, Galveston, TX 77552 in connection with its response to a recent data event discussed below. The purpose of this letter is to notify you of the event in accordance with Nebraska data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SES 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.

1. Nature of the Security Event

SES became aware of suspicious activity within its environment. Upon becoming aware of this, it immediately began an investigation to confirm the security of its system and to determine the nature and scope of this event. The investigation subsequently revealed certain information was acquired without authorization by an unknown actor.

SES then engaged cybersecurity specialists to conduct a thorough review of the affected data to determine whether it included personal information. On July 29, 2026, it confirmed the scope of the impact and secured information sufficient to effectuate notice.

Please note that it has no evidence of any actual or suspected misuse of information involved in this incident.

2. Number of Affected Nebraska Residents & Information Involved

The event involved personal information for approximately one Nebraska resident. The information involved in the event for the identified Nebraska resident included name, as well as driver's license or state identification number.

3. Notification to Identified Individuals

On July 31, 2026, a notification letter was sent to the identified Nebraska resident by USPS First Class Mail.

The notification letter provides resources and steps the individual can take to help protect their information. A sample notification letter is enclosed.

4. Measures Taken to Address the Event

Upon identifying this event, in addition to taking the steps described above, SES took steps to learn more about what happened and what information could have been affected. SES notified the identified individual and provided them with steps they can take to protect their personal information, including providing them with information about its toll-free call center through to answer questions about the event and to address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this event, please do not hesitate to contact me at NDaly@constangy.com.

Sincerely,

Nicholas Daly

Nicholas Daly
Partner, Constangy Cyber Team



0000216

Sullivan Environmental Services, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS4333

2_0000216



SULLIVAN ENVIRONMENTAL SERVICES



July 31, 2026

Subject: Notice of Data Security Event

Dear _____ :

We are writing to inform you about a data security event at Sullivan Environmental Services, Inc. (“SES”) that may have involved your personal information. We take the privacy and security of all personal information within our possession seriously. Please read this letter carefully as it contains details about the event and resources you can utilize to protect your information.

What Happened? SES became aware of suspicious activity within its environment. Upon becoming aware of this, we immediately began an investigation to confirm the security of our system and to determine the nature and scope of this event. The investigation subsequently revealed certain information was acquired without authorization by an unknown actor.

We then engaged cybersecurity specialists to conduct a thorough review of the affected data to determine whether it included personal information. On July 28, 2026, we confirmed the scope of the impact and secured information sufficient to effectuate notice.

Please note that we have no evidence of any actual or suspected misuse of information involved in this incident.

What Information Was Involved? The information that was potentially impacted during this incident may have included your name, as well as your

What Are We Doing. We take this incident and the security of data within our systems very seriously. Upon learning of this event, we moved quickly to ensure the security of our network and to fully understand the nature and scope of the event. We also worked with cybersecurity specialists to identify the impacted data and to whom it belongs. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

What Can You Do. Please review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions or need assistance, please contact 1-800-405-6108 Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Time, excluding major U.S. holidays. Cyberscout representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

Sullivan Environmental Services, Inc.
PO Box 17017
Galveston, TX 77552

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.

Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.

TransUnion, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional Information:

California: Office of the Attorney General, 1300 "I" Street, Sacramento, CA 95814-2919; 1-916-445-9555; <http://oag.ca.gov/>.

District of Columbia: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001; 1-202-727-3400; <https://oag.dc.gov/>.

Iowa: Office of the Attorney General of Iowa, 1305 E. Walnut Street, Des Moines, IA 50319; 1-888-777-4590; 1-515-281-5926; <https://www.iowaattorneygeneral.gov/>.

Kentucky: Office of the Attorney General, Capital Complex East, 1024 Capital Center Drive, Suite 200, Frankfort, KY 40601; 1-502-696-5300; <https://www.ag.ky.gov/>.

Maine: Office of the Maine Attorney General, 6 State House Station, Augusta, ME 04333; 1-207-626-8800; <https://www.maine.gov/ag/>.

Maryland: Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; <https://oag.maryland.gov/>.

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6000; <https://ncdoj.gov/>.

New York: New York State Attorney General, Bureau of Internet and Technology Resources, 28 Liberty Street, 15th Floor, New York, NY 10005; 1-800-771-7755; <https://ag.ny.gov/>.

Texas: The Texas Attorney General, 300 W. 15th Street, P.O. Box 12548, Austin, Texas 78711-2548; 1-800-621-0508; <https://www.texasattorneygeneral.gov/>.

Vermont: Attorney General's Office, 109 State Street, Montpelier, VT 05609, 1-800-649-2424, <https://ago.vermont.gov/>.