



David McMillan, Partner
Cybersecurity & Data Privacy Team
45 Main Street, Suite 206
Brooklyn, New York 11201
Telephone: 718.614.8371
Email: dmcmillan@constangy.com

August 29, 2025

VIA Online Submission

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

Re: **Notice of Data Security Incident**

Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Hutton Corporation (“Hutton”) in connection with a data security incident described in greater detail below. Hutton Corporation is a construction company headquartered in Wichita, Kansas. The purpose of this letter is to notify you of the impact to Nebraska residents in accordance with the Nebraska data breach notification statute.

1. Nature of the Security Incident

On August 7, 2025, Hutton discovered that it had experienced a network disruption and immediately initiated an investigation of the matter. Hutton engaged independent cybersecurity experts to assist with the process. As a result of the investigation, Hutton determined that certain files may have been acquired without authorization. Hutton undertook a comprehensive review of those files and, on or about August 15, 2025, learned that some of these files may have contained individuals’ personal information. Hutton then took steps to notify impacted individuals of the incident as quickly as possible.

Please note that Hutton has no current evidence to suggest misuse or attempted misuse of personal information involved.

2. Number of Affected Nebraska Residents & Information Involved

The incident involved personal information for approximately two Nebraska residents. The information involved in the incident may have included individuals’ names, Social Security numbers, Driver’s license numbers or other unique government-issued identification number, tax identification number, or IRS personal identification number.

3. Notification of Affected Individuals

On August 28, 2025, notification letters were mailed to affected Nebraska residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers 24 months of complimentary identity protection services to each individual whose personal information was affected by this event, including credit monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered by TransUnion – a leader in consumer identity protection. These services include: 12 months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken to Address the Incident

In response to the incident, Hutton retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Hutton also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

Hutton additionally notified the FBI's Internet Crime Complaint Center of this incident and will cooperate with any resulting investigation.

Finally, Hutton is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

4. Contact Information

Hutton remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at dmcmillan@constangy.com or 718.614.8371.

Sincerely,



David McMillan of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter



0000829

Hutton Corporation
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1717

5 0000829



To Enroll, Please Visit:

<https://bfs.cyberscout.com/activate>

Enrollment Code: [REDACTED]



August 28, 2025

Subject: Notice of Data Security Incident

Dear [REDACTED]:

We are writing to inform you of a recent data security incident at Hutton Corporation (“Hutton”) that may have affected your personal information. Hutton takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On August 7, 2025, Hutton discovered that it had experienced a network disruption and immediately initiated an investigation of the matter. Hutton engaged independent cybersecurity experts to assist with the process. As a result of the investigation, Hutton determined that certain files may have been acquired without authorization. Hutton undertook a comprehensive review of those files and, on or about August 15, 2025, learned that some of your personal information may have been contained within the potentially affected data which is the reason for this notification. Please note that Hutton has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name and Social Security number, Driver's license number or other unique government-issued identification number.

What We Are Doing. As soon as Hutton discovered this incident, it took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. Hutton is also offering you complimentary identity protection services through TransUnion, a leader in consumer identity protection. These services include 24 months of credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is 90 days from the date of this letter.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. 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.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-405-6108, Monday through Friday from 8:00 am to 8:00 pm Eastern time, excluding major U.S holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Steps You Can Take To Help Protect Your Personal 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 (the "FTC").

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 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
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 Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Kansas Attorney General

120 SW 10th Ave, 2nd Floor
Topeka, KS 66612
<https://www.ag.ks.gov/divisions/public-protection/consumer-protection>
785-296-2215

Oklahoma Attorney General

313 NE 21st Street
Oklahoma City, OK 73105
<https://oklahoma.gov/oag/about/divisions/cpu.html>
405-521-3921

Texas Attorney General

300 W 15th Street, Suite 9
Austin, TX 78701
<https://www.texasattorneygeneral.gov/consumer-protection>
512-463-2070

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.