



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

July 18, 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

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Davis, Hatley, Haffeman & Tighe, P.C. (“Davis Hatley”) in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On November 29, 2024, Davis Hatley became aware of unusual activity that disrupted access to some of its network resources. Upon discovering this activity, Davis Hatley immediately took steps to secure the network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation determined that the incident was due to a malicious encryption attack perpetrated by unknown actors, who gained access to the firm’s IT environment and potentially acquired certain files. On June 20, 2025, following a comprehensive review of those files, the firm confirmed that personal information belonging to certain individuals may have been impacted during the incident.

Davis Hatley is notifying all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

Please note that the firm has no evidence to suggest misuse or attempted misuse of any personal information in conjunction with this incident.

2. Number of Nebraska residents affected.

Davis Hatley notified 5 Nebraska residents of this incident via first-class U.S. mail on July 18, 2025. The information potentially impacted in connection with this incident includes names, Social Security numbers, driver’s license numbers, passport numbers, medical information, health insurance information, and dates of birth.

13167251v1
13180942v1

A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Davis Hatley discovered this incident, the firm took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, Davis Hatley implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. Davis Hatley also reported the incident to the FBI and will cooperate with any resulting investigation.

Davis Hatley has established a toll-free call center through TransUnion, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-(833)-380-8307 from 6:00 A.M. to 6:00 P.M. MT on Monday through Friday. In addition, while Davis Hatley is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Hatley is also providing complimentary credit and identity protection services to notified individuals.

4. Contact information.

Davis Hatley remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

/s/ David McMillan

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Davis, Hatley, Haffeman & Tighe, P.C.
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>



<< FirstName>> << LastName>>
<< Address1>>
<< Address2>>
<< City>>, << State>> << PostalCode+4>>

Subject: Notice of << Custom Field 1>>

Dear << FirstName>> << LastName>>:

Davis, Hatley, Haffeman & Tighe, P.C. ("Davis Hatley") is writing to inform you about a data security incident that may have involved your personal information. Davis Hatley takes the privacy and security of all information within its possession very seriously. Therefore, we are writing to inform you about the incident and advise you of certain steps you can take to help protect your personal information, including activating the free credit and identity monitoring services we are offering to you.

What Happened: On November 29, 2024, we became aware of unusual activity that disrupted access to some of our network resources. Upon discovering this activity, we immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation determined that the incident was due to a malicious encryption attack perpetrated by unknown actors, who gained unauthorized access to our IT environment and potentially acquired certain files. On June 20, 2025, following a comprehensive review of the affected files, we confirmed that your personal information was potentially impacted as a result of the incident.

What Information Was Involved? The information involved in this incident includes your name, as well as your << Exposed Data Elements>>. Please note that Davis Hatley has no evidence of any actual or suspected misuse of this information.

What We Are Doing: As soon as we discovered this incident, we took steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. In addition, we have implemented several technical measures in our environment to bolster Davis Hatley's security posture and reduce the chances of a similar incident occurring again. We also reported the incident to the FBI and will provide whatever assistance is necessary to help hold the perpetrators accountable.

In addition, we are also offering you 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 << service length>> 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. This service helps detect possible misuse of your information and provides you with identity protection support. The deadline to enroll in these services is 90 days from the date on this letter.

What You Can Do: 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: <Unique Code>. 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.

We encourage you to enroll in Cyberscout's complimentary identity protection services by going to the link noted above. Please also 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 [DEDICTED LINE], Monday through Friday from 6:00 a.m. to 6:00 p.m. Mountain Time, excluding major U.S. holidays. Cyberscout representatives are available for 90 days from the date of this letter and are fully versed on this incident and can help answer questions you may have.

Davis Hatley takes this situation extremely seriously and regrets any worry or inconvenience this may cause.

Very truly yours,

Davis, Hatley, Haffeman & Tighe, P.C

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

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers
877-566-7226

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.