



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

May 29, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs & Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

Constangy Brooks Smith & Prophete LLP represents Hardin, Kundla, McKeon & Poletto P.C. in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

Hardin, Kundla, McKeon & Poletto recently learned that certain personal information may have been subject to unauthorized acquisition in connection with a data security incident. After discovering suspicious activity in its network, Hardin, Kundla, McKeon & Poletto immediately initiated an investigation of the matter, engaging independent cybersecurity experts to assist with the process. As a result of this investigation, Hardin, Kundla, McKeon & Poletto determined that certain data stored in its network may have been acquired without authorization in or around January 2024. Hardin, Kundla, McKeon & Poletto undertook a comprehensive review of the affected data to determine whether any personal information may have been involved. Following this review, which concluded on March 31, 2025, Hardin, Kundla, McKeon & Poletto worked diligently to arrange for notification to potentially impacted individuals.

The information that may have been affected by this incident varies by individual, but includes individuals' names, dates of birth, usernames and associated passwords, medical information, health insurance information, driver's license and state ID numbers, passport numbers, government ID numbers, financial account numbers, tax ID numbers, biometric identifiers, and/or Social Security numbers. Please note, Hardin, Kundla, McKeon & Poletto has no evidence of the misuse or attempted misuse of any potentially impacted information.

2. Number of Nebraska residents notified.

Hardin, Kundla, McKeon & Poletto notified twenty-six (26) Nebraska residents of this incident via first class U.S. mail on May 29, 2025. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Hardin, Kundla, McKeon & Poletto discovered this incident, it took steps to secure its digital environment and launched an investigation to determine whether personal information had been accessed or acquired without authorization. Hardin, Kundla, McKeon & Poletto has also implemented additional safeguards to help ensure the security of its environment and to reduce the risk of a similar incident occurring in the future.

Hardin, Kundla, McKeon & Poletto 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. In addition, while Hardin, Kundla, McKeon & Poletto is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Hardin, Kundla, McKeon & Poletto is also providing complimentary identity protection services to individuals whose Social Security numbers were affected by the incident.

4. Contact information.

Hardin, Kundla, McKeon & Poletto 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.

Sincerely,

A handwritten signature in black ink, appearing to read "D. McMillan", followed by a horizontal line extending to the right.

David McMillan
Partner, Cybersecurity & Data Privacy Team

Enclosure: Sample Notification Letter

Hardin, Kundla, McKeon & Poletto, P.C.
579 Stoney Landing Road
Moncks Corner, SC 29461



To Enroll, Please Visit:

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

Enrollment Code: [REDACTED]



May 29, 2025

Subject: Notice of Data Security Incident

Dear [REDACTED],

We are writing to inform you about a data security incident that may have affected your personal information. Hardin, Kundla, McKeon & Poletto, P.C., takes the privacy and security of all information in its possession very seriously. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened: On March 31, 2025, Hardin, Kundla, McKeon & Poletto learned that some of your personal information may have been affected by a data security incident. The incident involved a malicious encryption attack perpetrated by unknown actors, resulting in certain files being copied from our network without authorization in or around January 2024. Hardin, Kundla, McKeon & Poletto engaged a team of leading cybersecurity experts to investigate the matter and help determine whether any sensitive data was included in the impacted files. Following a comprehensive review of the affected data, we learned that your personal information may have been involved in this incident. Please note that we have no evidence of the misuse of any of this information.

What Information Was Involved: The information that was potentially involved in this incident included your name and [REDACTED].

What We Are Doing: As soon as Hardin, Kundla, McKeon & Poletto discovered this incident, we took the steps described above and implemented measures to enhance the security of our computer environment and minimize the risk of a similar incident occurring in the future. In addition, we are also offering you [REDACTED] months of complimentary identity protection services through Cyberscout, a Transunion company. 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: We encourage you to enroll in Cyberscout's complimentary identity protection services by going to the link noted above. You can also follow the recommendations included with this letter to help protect your information.

For More Information: If you have any questions regarding this incident or need assistance, please do not hesitate to call **1-833-566-5782** Monday through Friday between 8 am and 8 pm Eastern, excluding holidays. Cyberscout agents are well versed in this incident and can answer any questions you may have.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Hardin, Kundla, McKeon, & Poletto
673 Morris Avenue
Springfield, NJ 07081

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

New Jersey State Police

Office of the Superintendent
P.O. Box 7068
West Trenton, NJ 08628
1-833-4-NJCCIC



Rhode Island: A total of 12,063 individuals were notified of this incident.

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.