CONSTANGY
Brooks Smith & Prophete

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

Bert Bender, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, 36th Floor
Philadelphia, PA 19103
bbender@constangy.com
Direct: 445-308-1588

February 11, 2026

Via Portal Submission Only
Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

Re: Notice of Data Event

Dear Attorney General Hilgers,

Constangy, Brooks, Smith & Prophete LLP represents McDonnell Capital Management located at 19550 S. Harlem Avenue, Suite 3, Frankfort, IL 60423 in connection with a recent incident described below. The purpose of this letter is to notify you of the incident and provide with a summary of the response thereto. McDonnell Capital Management does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, personal jurisdiction, or any other potentially applicable rights or defenses by providing this notice.

1. Nature of the Security Incident.

McDonnell Capital Management learned of the event on September 4, 2025, when it identified suspicious activity related to an employee's email account. McDonnell Capital Management immediately investigated with assistance from cybersecurity specialists and determined an unauthorized individual accessed the employee's account between August 29, 2025 and September 3, 2025. The investigation determined emails were accessed during the window of access, so McDonnell Capital Management conducted a comprehensive review of the accessed emails to identify the specific information present in these emails so it could notify individuals as appropriate. This email review ended on December 8, 2025, after which McDonnell Capital Management continued to review and to reconcile records so it could confirm applicable address information and notify individuals as needed.

On February 4, 2026, McDonnell Capital Management completed its address reconciliation and confirmed there were four Nebraska residents whose information was in the accessed emails. McDonnell Capital Management has no current evidence any information was used to further identity theft or fraud.

2. Notice to Nebraska Residents

McDonnell Capital Management notified four Nebraska residents of this incident via first-class U.S. mail on February 11, 2026. The information in the accessed emails varied by individual but may include individual name, Social Security number, and financial account information.

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

3. Steps Taken Relating to the Incident.

McDonnell Capital Management took steps to secure its email environment after learning of the incident. It also conducted a comprehensive review to determine the scope of personal information accessible due to the incident. In addition, McDonnell Capital Management implemented measures to enhance the security of information in its care and continue to assess and to implement steps in response to the incident as appropriate.

McDonnell Capital Management notified all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering them access to complimentary identity monitoring services. McDonnell Capital Management also established a dedicated call center to answer any questions about the incident and address related concerns.

4. Contact Information.

McDonnell Capital Management remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please contact us.

Best regards,

Robert H. R[illegible]

Bert Bender
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Encl.: Sample Consumer Notification Letter

McDonnell Capital Management
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2786

0000006

[redacted]

[redacted]

February 11, 2026

Re: NOTICE OF DATA EVENT

Dear [redacted],

We are writing to inform you of an event that may have an impact on the confidentiality of some of your information. McDonnell Capital Management values the privacy and security of all information in our care and this letter provides information about the event, our response, and steps you may take to further protect your personal information, should you determine it is appropriate to do so.

What Happened? On December 8, 2025, we determined some of your information was accessed during the recent event. We learned of the event on September 4, 2025, when we discovered suspicious activity related to an employee's email account. We immediately investigated with assistance from cybersecurity specialists and determined an unauthorized individual accessed the mailbox between August 29, 2025 and September 3, 2025. We also reviewed the emails that were accessible to the unauthorized individuals to determine the specific information present in these emails so we could notify individuals as appropriate. This process ended on December 8, 2025, which is when we determined the specific information accessed within the mailbox. We then confirmed available address information so we could notify individuals, including yourself.

What Information Was Involved? The personal information in the mailbox included [redacted]. The information in the mailbox was in documents that had been sent to us via email. We have no evidence any of this information was used to facilitate identity theft or fraud.

What We Are Doing. Upon discovery of this event, we immediately investigated to determine the full nature and scope of this event and to assess the security of our network. As part of our ongoing commitment to the privacy of information within our care, we implemented additional security measures to further protect against similar incidents in the future. For example, we no longer accept certain customer information via email and we are restricting the process for sharing any documents with sensitive information.

We are providing you with 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 12 months 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.

If you wish to receive these services, you must enroll by following the below enrollment instructions as we are unable to activate these services on your behalf. 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.

What You Can Do. We encourage you to remain vigilant against events of identity theft and fraud and to review your accounts statements and credit reports for the next 24 months to detect errors or suspicious activity. You should report any suspicious information to your financial institution or law enforcement as appropriate. You can find more information about protecting yourself against potential identity theft and fraud, and other resources available to you in the enclosed attachment. You may also enroll in the complimentary credit monitoring services available to you at no cost.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. You can contact us at contact our dedicated call center at 1-800-405-6108 with any questions.

Sincerely,

McDonnell Capital Management

0000006

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.

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 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

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. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/credit-freeze.

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

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

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

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

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

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

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

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

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.