GODFREY & KAHN

833 EAST MICHIGAN STREET, SUITE 1800
MILWAUKEE, WISCONSIN 53202-5615

TEL • 414.273.3500 FAX • 414.273.5198

WWW • GKLAW.COM

Direct: 414.287.9495
AFarrell@gklaw.com

May 29, 2026

VIA ONLINE SUBMISSION

Attorney General Brenna Bird
Hoover Building
1305 E. Walnut Street
Des Moines, IA 50319

RE: Data Incident Notification

Dear Attorney General Bird:

Our firm represents KerberRose S.C. ("KR"), a Wisconsin company. On behalf of itself and Natural Beauty Growers, LLC, KR hereby formally submits notification of a recent data incident pursuant to Iowa Code § 715C.1-2. KR reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, KR does not waive any rights or defenses regarding the applicability of Iowa law, including the applicability of Iowa Code § 715C.1-2, the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over KR.

On May 1, 2026, KR became aware that an unauthorized third party had gained access to an email account of one KR employee on April 29, 2026, that resulted in limited access to a portion of a back-up platform used in operating KR's wealth management business. No other systems and no other divisions of KR's business were impacted. Importantly, the CPA and tax services offered through KR were unaffected. Immediately upon learning of the incident, KR took steps the same day to isolate the impacted environment. KR also began an investigation with the help of a leading forensic security firm that specializes in data security incidents to assist in mitigation efforts and to secure the environment. As part of the investigation, KR worked to identify who may have been impacted by this incident and what personal information may have been accessed and/or acquired by the third party. The information impacted generally included names, addresses, Social Security numbers, financial account numbers, bank account information, and dates of birth. At this time, KR does not have evidence that any fraud or identity theft has occurred as a result of this incident.

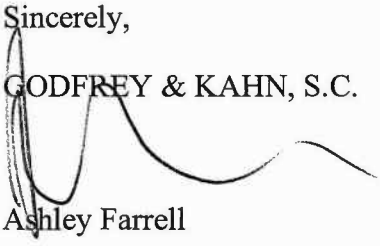
In light of the foregoing and out of an abundance of caution, KR has decided to notify your office (via this letter) and the 638 Iowa residents potentially affected by this incident via U.S. Mail on or about May 29, 2026. A sample of the notification letter is attached hereto as Exhibit A.

In addition to providing notice to you through this letter, KR took immediate steps once notified to assess, isolate, and mitigate the impact of the incident. In addition to conducting a full investigation, KR has also implemented additional administrative and technical safeguards and strengthened its password policies.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

GODFREY & KAHN, S.C.



Ashley Farrell

AF:cg
Attachment

EXHIBIT A

Sample Notification Letter

38425911.1

KerberRose Wealth Management, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

[redacted]

May 29, 2026

Notice of Data Breach

Dear [redacted]

At KerberRose Wealth Management, LLC ("KerberRose"), we take the privacy and security of our customers' personal information seriously. For that reason, we are writing to provide you with notice of a recent data security incident experienced by KerberRose that involved your personal information. We are notifying you of this incident because you are either a wealth management customer of KerberRose or an applicant for or participant (or an alternate payee of the participant) in a retirement plan for which KerberRose provides services. While KerberRose does not have any evidence at this time that your personal information has been used in a fraudulent way, we take this matter seriously and are nonetheless sending this letter to:

- **Communicate what happened**
- **Identify the personal information involved**
- **Provide details on how to enroll in 24-months of identity monitoring and theft resolution services we are offering to you at no charge**

What Happened

On May 1, 2026, KerberRose became aware that an unauthorized third party had gained access to an email account of one employee on April 29, 2026, that resulted in limited access to a portion of a back-up platform used in operating KerberRose's wealth management business. No other systems and no other divisions of KerberRose's business were impacted. Importantly, the CPA and tax services offered through KerberRose S.C. were unaffected. Immediately upon learning of the incident, KerberRose took steps the same day to isolate the impacted environment. KerberRose also began an investigation with the help of a leading forensic security firm that specializes in data security incidents to assist in mitigation efforts and to secure the environment. As part of the investigation, KerberRose worked to identify who may have been impacted by this incident and what personal information may have been accessed and/or acquired by the unauthorized third party. Please note that this notice was not delayed by law enforcement.

What Personal Information Was Involved

The personal information involved may have included your name, address, Social Security number, financial account numbers, bank account information and date of birth.

Please note, however, that neither KerberRose nor its forensic security firm have found any evidence at this time that any of your personally identifiable information has been used in a fraudulent way.

What We Are Doing

In addition to providing notice to you through this letter, KerberRose took immediate action to investigate and contain this incident and work with experts experienced in handling security incidents. Additionally, to help protect your identity, 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 24 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 the event that you become a victim of fraud. These identity monitoring services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

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.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-877-426-6807 and supply the fraud specialist with your unique code listed above.

Additional Steps You Can Take

To help protect your personal information, we strongly recommend you do the following:

- Carefully review your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS) statements. Notify the statement sender immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- Enroll in the identity monitoring service that we are offering you through Cyberscout, a TransUnion company.
- Additional steps and resources are available in the accompanying Reference Guide. We encourage you to read and follow these steps as well.

For More Information

If you have questions, concerns or learn of any suspicious activity that you believe may be related to this incident, please contact us at 1-920-785-8073. Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,

Anthony Powers

President of Wealth Management

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, or to obtain additional information about fraud alerts and security freezes, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place a Fraud Alert on Your Credit or Consumer File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-685-1111	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit or Consumer File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus.

The consumer reporting agencies may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at:

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

Please note additional guidance is available at usa.gov.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General at consumer@ag.iowa.gov, by calling (515) 281-5926, or writing to 1305 E. Walnut Street, Des Moines, IA 50319-0106.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, https://www.marylandattorneygeneral.gov/.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office

Bureau of Internet and Technology

(212) 416-8433

https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection

(800) 697-1220

https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services. [redacted] Rhode Island residents were impacted by this incident.