Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

March 13, 2026

Via Online Portal:

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Cybersecurity Incident Involving Kerkering, Barberio & Company

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Kerkering, Barberio & Co., Certified Public Accountants ("KB"), a CPA firm located in Sarasota, Florida, with respect to a recent data security incident that was first discovered on May 27, 2025 (hereinafter, the "Incident"). KB takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been affected, the number of Maine residents being notified, and the steps KB has taken in response to the Incident. We have also attached a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring and identity theft protection services.

1. Nature of the Incident

On or around May 27, 2025, KB discovered the Incident when it became aware of access to four (4) email accounts by an unauthorized user. Upon discovery of this incident, KB immediately isolated the affected email accounts and promptly engaged a specialized third-party cybersecurity firm to assist with securing the email accounts, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The preliminary forensic investigation found evidence that some KB files were obtained by an unauthorized actor.

Based on these findings, KB engaged a third-party data mining vendor to conduct a comprehensive review of the potentially accessed data to identify the individuals whose sensitive information was present within the impacted e-mail accounts at the time of the Incident. In addition, KB engaged a third-party notification vendor to assist with notifying the affected individuals. On March 6, 2026, KB finalized the list of individuals to notify.

Although KB is unaware of any fraudulent misuse of information, it is possible that individuals' address, email, Social Security Number, and full name may have been exposed as a result of this

unauthorized activity. As of this writing, KB has not received any reports of related identity theft since the date of the incident (May 27, 2025 to present).

2. Number of Maine residents affected.

Based on its investigation, KB determined that a total of three (3) Maine resident(s) may have been potentially affected by this incident. Notification letters to these individuals were mailed on March 13, 2026, by U.S. mail. A sample (redacted) copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Data privacy and security is among one of KB's highest priorities, and KB is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the incident, KB has moved quickly to investigate, respond, and confirm the security of our systems. Specifically, KB disconnected all access to the impacted email accounts, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps and will continue to take steps to mitigate the risk of future harm. Lastly, KB informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although KB is not aware of any actual or attempted misuse of the affected personal information, KB offered 12 (twelve) months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company, to all individuals to help protect their identity. Additionally, KB provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

KB remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Kerkering, Barberio & Company
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2642

0000851

6_0000851

[redacted]

March 13, 2026

Re: Notice of Data Security Incident

Dear [redacted],

Kerkering, Barberio & Company ("Kerkering") is writing to inform you of a recent data incident that may have resulted in an unauthorized access to your sensitive personal information. We are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On or around May 27, 2025, Kerkering became aware of access of four email accounts by an unauthorized actor. Upon discovery of this incident, Kerkering immediately isolated the affected email accounts and promptly engaged a specialized third-party cybersecurity firm to assist with securing the email accounts, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The preliminary forensic investigation found evidence that some Kerkering files were accessed by an unauthorized actor.

Based on these findings, Kerkering conducted an extensive review of the affected files to identify the specific individuals and the types of information that may have been compromised. On March 6, 2026, Kerkering finalized the list of individuals to notify.

What Information Was Involved?

Based on the investigation, the following information related to you may have been subject to unauthorized access: Bank Account Details, Credit Card (scan), Credit Card Cvc, Credit Card Expiry, Credit Card Number, Date of Birth, Driver Licence (scan), Driver Licence Expiry, Driver Licence Number, Email, Home Phone, Insurance Details, Login Access, Login Password, Login Username, Medical Reference Number, Mobile, Passport (scan), Passport Expiry, Passport Number, Private Health Member ID, Social Security Number, Trust Name, Trust Social Security Number and name.

What We Are Doing

Data privacy and security is among Kerkering's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, Kerkering has moved quickly to investigate, respond, and confirm the security of our systems. Specifically, Kerkering disconnected all access by the impacted business email to our network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

In response to the incident, 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. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Any taxpayer can proactively request an Identity Protection PIN to ensure no one else files their return without authorization. Instructions for obtaining an Identity Protection PIN are available at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

If your Social Security number is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these actions:

- Respond immediately to any IRS notice: Call the number provided.
- If your e-filed return is rejected because of a duplicate filing under your Social Security number, or if the IRS instructs you to do so, visit irs.gov/victimassistance to complete Form 14039, Identity Theft Affidavit, attach it to the back of your completed paper tax return and mail to the IRS location based upon the state you reside. You also have the option to submit the Form 14039 online and mail your paper return separately.
- Visit IdentityTheft.gov for steps you should take right away to protect yourself and your financial accounts.

If you need additional guidance with these steps, please contact the toll-free number in the *For More Information* section of this letter for assistance.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is 90 days from the date on the letter. 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 an 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

If you have any questions or concerns not addressed in this letter, please call 1-833-297-3832 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Kerkering sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

KERKERING, BARBERIO & COMPANY

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission (FTC)

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Internal Revenue Service (IRS)

Tax-related identity theft occurs when someone uses your stolen personal information, including your Social Security number, to file a tax return claiming a fraudulent refund. If you suspect you are a victim of identity theft, continue to pay your taxes and file your tax return, even if you must file a paper return. If your Social Security number is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these actions:

- Respond immediately to any IRS notice: Call the number provided.

- If your e-filed return is rejected because of a duplicate filing under your Social Security number, or if the IRS instructs you to do so, visit irs.gov/victimassistance to complete Form 14039, Identity Theft Affidavit, attach it to the back of your completed paper tax return and mail to the IRS location based upon the state you reside. If you prefer, you have the option to submit the Form 14039 online and mail your paper return separately.
- Visit IdentityTheft.gov for steps you should take right away to protect yourself and your financial accounts.

Our firm is committed to supporting you during this time. If you need additional guidance with these steps, please contact the toll-free number in the *For More Information* section of this letter for assistance.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx. Kerkering, Barberio & Company is located at 1605 Main Street #600, Sarasota, Florida 34236, and can be reached by phone at (941) 966-4617.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.