<<First Name>> <<Last Name >>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>



<<Date>>

Dear <<First Name>> <<Last Name >>,

McAdam Financial Group ("McAdam") is writing to inform you of a data security event that may impact certain information related to you. This information was collected based on the relationship you may have with your financial advisor [redacted] who was an employee (independent contractor) of McAdam at the time of the incident. As discussed further below, we take this matter seriously, and have been working with cybersecurity specialists to investigate and respond. As our diligent investigation is now complete, we are sending you this letter because certain information related to you may have been affected.

What Happened? In early April 2026 we detected unusual activity in one email account within our environment. We quickly took steps in response, including to secure the relevant account, and engage third-party specialists to conduct a comprehensive investigation. The investigation determined that only limited email items within one email account were accessed without authorization between March 30 and March 31, 2026. Accordingly, we conducted a thorough review of the relevant email items in the one email account to determine the specific information present and to whom the information related. The preliminary results of the diligent review process were completed on May 11, 2026. Thereafter, we continued our efforts to further review, identify necessary contact information, and align resources for notification, all of which was completed on June 9, 2026. As certain information related to you was identified within the relevant data, we are providing you with this notification.

What Information Was Involved? Our review identified the following information related to you may have been accessed in connection with this matter: name and Social Security number.

What Did We Do In Response? In response to this event, we took steps to secure the relevant account in our email environment and conducted a comprehensive investigation, which was aided by third-party forensic specialists. Once the information that may have been impacted was confirmed, we diligently reviewed the information and to whom it related in order to assess potential notification obligations. As the obligation to safeguard the information in our care is of paramount importance to us, we are implementing additional security measures to further enhance our cybersecurity infrastructure, as well as revising and implementing additional policies and procedures regarding data and providing training to our workforce with a goal of minimizing the risk of a future similar incident.

What You Can Do. As an added measure, in an abundance of caution, McAdam is offering you complimentary credit monitoring for twelve (12) months through TransUnion. Please note, we cannot enroll you in these services, however, if you would like to enroll, information and instructions are included in this letter. It is also recommended that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is recommended that you promptly contact the financial institution or credit/debit card issuing company. Additional information and resources are outlined in the *Steps You Can Take to Help Protect Your Information* section of the letter below.

For More Information. We understand that you may have additional questions about this letter. Should you have any questions or concerns, please contact us by email at [redacted] or by phone at [redacted]. Please know that we take this matter and the obligation to safeguard the information in our care very seriously and we are taking additional steps to further bolster our environment and existing cybersecurity protocols.

Sincerely,
McAdam Financial Group

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Offered Monitoring Services

In response to the incident, we are providing you with access to twelve (12) months of complimentary Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score monitoring 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. Notifications are sent the same day that a change or update takes place with the bureau. Moreover, with the services include 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.

How do I enroll for the free 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: <CODE HERE>

Please note, in order for you to receive the monitoring services described above, you must enroll before January 11, 2027. 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. McAdam Financial Group & McAdam LLC. 150 N. Radnor Chester Road, Suite F200 Radnor, PA 19087.