



SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
+1 202 736 8000
+1 202 736 8711 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 202 736 8477
ARAUL@SIDLEY.COM

August 31, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Security Incident Notification

Dear Attorney General Anthony G. Brown,

On behalf of our client, Marathon Asset Management, L.P. (“Marathon”), we are writing to notify you about a data security incident that may have involved personal information related to 6 Maryland residents. At this time, we have no indication of fraud or misuse of Marathon personal information as a result of this incident.

As explained in the enclosed notice to potentially impacted individuals, on October 18, 2022, a law firm notified Marathon that its vendor (AMS File Transfer) experienced a data security incident that may have resulted in unauthorized access to investor subscription agreements. The law firm represented a lender to one of Marathon’s investment funds, and reviewed the subscription agreements in connection with the loan. The law firm told us that, upon discovering the incident, it and its vendor promptly hired forensic experts to investigate the nature and scope of the incident, and notified federal law enforcement. Although the investigation did not identify any evidence that personal information was stolen or misused as a result of this incident, the investigation could not conclusively rule out that the unauthorized individual accessed or acquired Marathon personal information.

Marathon has notified 6 Maryland residents whose personal information may have been made available as a result of the security incident. The personal information that may have been impacted included name, Social Security number, financial account number, date of birth, driver’s license number, and/or passport number. Attached is a sample copy of the notification.

Upon receiving notice of the incident from the law firm, Marathon took prompt steps to investigate the nature and scope of the incident, and gain assurances from the law firm and its vendor that all Marathon personal information has since been deleted from their systems. Marathon also understands that AMS File Transfer has added additional security features to its systems to protect against future incidents.

If you have any questions, please do not hesitate to contact me.

Sincerely,

/s/ Alan Charles Raul

Alan Charles Raul
Partner



<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

<<Date>>

NOTICE OF DATA SECURITY INCIDENT

Dear <<Name 1>> <<Name 2>>:

We are writing to notify you of an incident that may have involved your personal information. At this time, we have no indication of fraud or misuse of your personal information as a result of this incident. Nevertheless, we are notifying you to explain the circumstances as we understand them, and to make you aware of the steps we have taken to respond and the resources we are making available to you.

What Happened?

On October 18, 2022, a law firm representing a lender to Marathon Distressed Credit Fund notified us that a vendor providing services to such law firm (AMS File Transfer) experienced a data security incident that may have resulted in unauthorized access to your subscription agreement. The law firm reviewed the subscription agreements in connection with the loan. The law firm told us that, upon discovering the incident in early August, it and its vendor hired forensic experts to investigate the nature and scope of the incident, and notified federal law enforcement. The attack appears to have taken place in September 2021, and then again in January 2022. Although the investigation did not identify any evidence that your personal information was stolen or misused as a result of this incident, the investigation could not conclusively rule out that the unauthorized individual accessed or acquired your personal information.

What Information Was Involved?

The personal information relating to you that may have been affected by this incident is the personal information that you submitted in connection with your subscription documents, which may include, as applicable, your name and Social Security number, financial account number, date of birth, driver's license number, and/or passport number.

What We Are Doing.

Upon notice from the law firm, we took prompt steps to investigate the nature and scope of the incident, and gain assurances from it and its vendor that all of your personal information has since been deleted from their systems.

What You Can Do.

We encourage you to remain vigilant with respect to your personal accounts, as appropriate. Additional information and resources are included in the enclosed "Steps You Can Take To Protect Personal Information."

For More Information.

If you have additional questions, please contact us at dataprivacy@marathonfund.com or (212) 500-3080.

Sincerely,

Jason Friedman
Partner



STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); 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 credit freeze, please contact the three major credit reporting bureaus listed below:

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

Additional Information

Federal regulatory agencies recommend that you remain vigilant for the next 12 to 24 months and report any suspected incidents of fraud to your relevant financial institutions.



You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 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 and your state Attorney General. This notice has not been delayed by law enforcement.

Special Information for Residents of Maryland, North Carolina, and Oregon

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.