



Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David B. Sherman
direct dial: 215.564.8380
dsherman@bakerlaw.com

June 28, 2023

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of our client, School Specialty, LLC (“School Specialty”) to notify your office of a cybersecurity incident experienced by one of School Specialty’s former third-party vendors, The Management Association (“MRA”), that involved eight Maryland residents’ information. School Specialty is headquartered in Greenville, WI.

On May 14, 2024, MRA reported to School Specialty that it experienced a ransomware incident. School Specialty previously partnered with MRA who provided human resources consultation services to School Specialty. MRA reported that on July 29, 2023, it discovered a cybersecurity incident. MRA’s investigation determined that an unauthorized user gained access to its network and took certain files from its servers, including files that contained information associated with current or former School Specialty employees. MRA reviewed the files, and on June 11, 2024, MRA identified eight Maryland residents whose names and Social Security numbers were involved.

On June 28, 2024, MRA will mail notification letters via United States Postal Service First-Class mail to the involved Maryland residents in accordance with Md. Code Ann., Com. Law § 14-3504. A sample copy of the notification letter is enclosed. MRA is offering the Maryland residents a one-year complimentary membership to credit monitoring and identity protection services through IDX. MRA has also established a dedicated, toll-free call center to answer questions the letter recipients may have.

June 28, 2023

Page 2

MRA informed School Specialty that MRA has implemented additional technical safeguards to improve the security of its environment.

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

Sincerely,

A handwritten signature in dark ink, appearing to read "David B. Sherman". The signature is fluid and cursive, with a large initial "D" and "S".

David B. Sherman
Partner

Enclosure

MRA – The Management Association
Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:




Or Visit

<https://app.idx.us/account-creation/protect>

June 28, 2024

<<(For CA Residents Only) Notice of Data Breach>>

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

I am writing to inform you of a security incident experienced by MRA involving some of your information. MRA was in possession of your information in the regular course of business and in connection with services performed on behalf of <<Business Name>>. We are providing you with information about the incident, our response, and steps you can take to protect your information.

What Happened? <<On July 29, 2023, MRA experienced a network disruption. Upon discovery / MRA experienced a network disruption and upon discovery>>, we locked down our systems. We immediately launched an internal investigation and engaged cybersecurity firms to assist with our investigation and response. This investigation ultimately confirmed that to certain information maintained by MRA was accessed by an unauthorized party. We conducted a thorough review with the assistance of third-party specialists to determine the information involved. We subsequently worked to confirm appropriate contact information and notify <<Business Name>>, which was completed on June 11, 2024.

What Information Was Involved? The information potentially impacted during the incident included your name in combination with the following data elements: <<Data Elements>>.

What Are We Doing? We take this incident seriously and apologize for any concerns this may cause. In response to this incident, we are providing you with access to <<12/24>> months of credit monitoring and identity protection services at no cost to you. While we already had several security measures in place and regularly undertake independent security audits, MRA has implemented additional technical safeguards and works with outside specialists to continually monitor all our systems.

What You Can Do. We encourage you to enroll in the credit monitoring and identity protection services we are making available to you. Instructions about how to enroll in these services and additional steps you can take are included in the additional pages of this letter.

For More Information: Any questions related to this incident can be directed to our dedicated assistance line at 1-888-804-6203 between 8 am – 8 pm Central Time, Monday through Friday excluding U.S. holidays.

We sincerely appreciate your understanding in this matter.

Sincerely,

Susan Fronk
President & CEO

Steps You Can Take to Protect Your Information

1. Website and Enrollment. Scan the QR image, go to <https://app.idx.us/account-creation/protect>, or call 1-888-804-6203 and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. IDX representatives are available Monday through Friday from 8 am – 8 pm Central Time. Please note that the deadline to enroll is September 28, 2024. IDX Identity enrollments will include enrollments into the following service components:

CREDIT MONITORING (adults¹) - Monitoring of credit bureau for changes to the member's credit file such as new credit inquiries, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY – IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to) account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage the restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-804-6203 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months. 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. Contact the credit reporting bureau if you have questions or notice incorrect information.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team, who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, and the FTC.

¹ Please note that these services are only available to those aged 18 years or older.

Monitor Your Accounts

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 placed on a consumer's credit file. Upon seeing a fraud alert, a business must 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.

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/>. MRA - The Management Association may be contacted at N19W24350 Riverwood Drive, Waukesha, WI 53188.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators.

You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. <<#>> residents of Rhode Island have been affected by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. MRA - The Management Association may be contacted at N19W24350 Riverwood Drive, Waukesha, WI 53188.