



January 30, 2023

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

Via Online Portal

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

Re: Supplemental Notice of Data Security Incident
Client: Homeschool Legal Defense Association
File No.: 15991.01190

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman & Dicker LLP (“Wilson Elser”) represents Homeschool Legal Defense Association (“HSLDA”), headquartered in Purcellville, Virginia with respect to a recent data security incident. HSLDA is a non-profit organization providing non-legal services to families who homeschool their children. HSLDA takes this matter very seriously and is taking measures to remediate the incident and has provides notice to potentially affected individuals.

This letter will serve to supplement our prior notice with regards to this incident submitted to your office on March 4, 2022, and inform you of additional information regarding the nature of the incident, the number of additional Maine residents being notified, and further steps that HSLDA has taken in response to the incident.

1. Nature of the incident.

On February 2, 2022, HSLDA was notified by a third-party service provider of suspicious activity involving its payroll management system. Immediately upon notification, HSLDA took steps to mitigate the impact of the incident by shutting down access to the payroll system, changing passwords, and engaging third party experts to assist in remediation steps. Additionally, HSLDA commenced an investigation to determine the nature and scope of the incident. The investigation revealed that an unauthorized party gained access to HSLDA’s payroll system using compromised credentials. While the investigation was unable to confirm the specific employee information that may have been accessed, HSLDA provided notice to all employees, regardless of whether their information was confirmed to be subject to unauthorized access or acquisition.

Upon completing the first round of notification, HSLDA subsequently engaged a third-party data mining vendor to conduct a further review of the information that may have been involved in the incident. Upon completion of its investigation, HSLDA discovered that additional individuals may have been impacted by the incident. HSLDA has since worked to identify the individuals whose information may have been involved in the incident. On January 19, 2023, HSLDA provided a second round of notice to the additional individuals whose information was affected as a result of the incident.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

2. Number of Maine residents affected.

HSLDA discovered that an additional five (5) residents of Maine were impacted by this incident. Notification letters were sent to these individuals on January 19, 2023. A sample notice letter that was sent to the impacted individuals is included as **Exhibit A**.

3. Steps taken.

HSLDA takes the security of personal information in its control very seriously, and has taken steps to prevent a similar event from occurring in the future, including but not limited to: strengthened internal password policy by increasing complexity and enhanced secure login authentication procedures for third party service provider accounts.

Further, HSLDA has provided the individuals whose PII was potentially accessed by an unauthorized individual with twelve (12) months of unlimited access to their Equifax credit report and credit score as well as a daily credit monitoring service that will notify the individual if there are any critical changes to their credit file at Equifax. The services provided also include access to an identity restoration program that provides assistance in the event that an individual's identity is compromised to help them restore their identity and up to \$1,000,000 in identity theft insurance.

4. Contact information.

HSLDA 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

Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

We are writing to inform you of a data security incident which affected Homeschool Legal Defense Association (“HSLDA”), a non-profit organization dedicated to assisting families with homeschooling services located in Purcellville, Virginia. The data security incident may have impacted some of your personal data. This letter contains information about the incident and information about how to protect your personal information going forward. HSLDA considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident. At this time, we have no indication that your information has been misused.

What Happened

On February 2, 2022, HSLDA was notified by one of our third-party service providers of suspicious activity involving our payroll management system. Immediately upon notification, we took steps to mitigate further harm by shutting down access to the payroll system, changing passwords, and engaging third party experts to assist in remediation steps. Additionally, HSLDA commenced an investigation to determine the nature and scope of the incident. The investigation revealed that an unauthorized party gained access to HSLDA’s payroll system using compromised credentials. While the investigation was unable to confirm the specific employee information that may have been accessed, HSLDA provided notice to all employees, regardless of whether their information was confirmed to be subject to unauthorized access or acquisition.

Upon completing the first round of notification, HSLDA engaged a third-party data mining vendor to conduct a further review of the information that may have been involved in the incident. Upon completion of its investigation, HSLDA discovered that additional individuals may have been impacted by the incident. HSLDA has since worked to provide notice to all individuals whose information may have been impacted as result of the incident.

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to <<Affected Data>>.

What We Are Doing

The security and privacy of your personal information contained within HSLDA systems is a top priority, and HSLDA is taking additional measures to protect this information. Since the incident, HSLDA has continued to strengthen its security posture by adding security controls, including strengthening its internal password policy by increasing complexity and enhancing secure login authentication procedures for third party service provider accounts.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (1-Bureau Credit Watch Gold) for twelve (12) months provided by Equifax, one of the three nationwide credit reporting companies.

You can sign up for the credit monitoring service anytime between now and **April 30th 2023**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain twelve (12) months of unlimited access to your Equifax credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

How Do I Enroll for the Free Services?

To enroll in this service, go to the Equifax website at www.equifax.com/activate and in the space referenced as “Enter Activation Code”, enter the following Activation Code <<Activation Code>> and follow the steps to receive your credit monitoring service. Please see more information regarding the enrollment process at the end of this letter.

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. 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 Important Information*, to learn more about how to protect against the possibility of information misuse.

The protection of your personal information is a top priority and we sincerely regret any concern or inconvenience this matter may cause. If you have any questions, please do not hesitate to call **1-855-962-3266** Monday through Friday, between 9:00 AM and 9:00 PM, Eastern Time.

Sincerely,



Charles L. Hurst
VP of Administration
Homeschool Legal Defense Association

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for

your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
(800)-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
(888)-397-3742

www.experian.com/freeze

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
(800)-680-7289

freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.