GREGORY N. BRESCIA

MARK ISHMAN

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
500 MAMARONECK AVE, SUITE 503
HARISSON, NY 10528
WWW.GRSM.COM

November 15, 2024

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)
Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident
Our File No: 1362061

To Whom It May Concern:

Our client, ESHA, Inc ("ESHA"), a revenue cycle management company, understands the importance of protecting personal information and is making this notification to your Office in accordance with applicable law following a recent data security incident.

On July 19, 2024, ESHA became aware of a data security incident that impacted its server infrastructure and took its systems offline. ESHA immediately undertook efforts to restore its servers and undertook additional affirmative steps to safeguard the security of data maintained on its systems. ESHA also simultaneously retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.

In accordance with ESHA's business associate agreements with the covered entities, on September 17, 2024, ESHA issued notification letters. Within the notification letters, ESHA provided a summary of the security incident inclusive of the mitigation and restoration actions taken by ESHA as a result of the security incident. ESHA has also requested confirmation from the covered entities as to whether or not they elect to delegate the duty to report the security incident to the individuals. To date, we have received confirmation from a select number of covered entities and intend to provide notice of the incident to all potentially impacted individuals by November 15, 2024.

The forensic investigation determined that access to ESHA's systems occurred on approximately July 13, 2024 through July 17, 2024. The investigation also identified certain files that may have been accessed or acquired in connection with the incident. In continuing its thorough investigation, ESHA undertook a comprehensive manual review process to review these files and identify the specific individuals with person information contained therein. This comprehensive manual review process concluded on or about September 16, 2024.

On or about August 5, 2024, the external forensic investigation firm confirmed that the data security involved the unauthorized access to ESHA's system. The forensic investigation confirmed that, during this brief period of unauthorized access, there was unauthorized access to and/or acquisition of certain files maintained on ESHA's systems. As a result, ESHA undertook a comprehensive and time intensive review of all files that may have been accessed and/or acquired in connection with the incident to determine the presence of any PII and/or PHI contained therein, as well as the associated practices and individuals, in order to comply with ESHA's obligations in connection with the incident. This comprehensive review process was completed on or about September 16, 2024, at which point ESHA determined that there was PII and/or PHI contained within the files that may have been accessed and/or acquired in connection with the incident.

As stated above, following the data security incident, ESHA immediately undertook all efforts to restore its servers, and also undertook additional affirmative steps to safeguard the security of data maintained on its systems. ESHA retained a forensic investigation firm to thoroughly investigate the incident and providing notification to all individuals whose personal information may have been accessed and/or acquired in connection with the incident in an abundance of caution. ESHA has obtained confirmation to the best of its ability that the information is no longer in possession of the third party(ies) associated with this incident, and it is entirely possible that any specific personal and/or protected health information *was not compromised* as a result of the incident. Nonetheless, ESHA has also offered to the impacted individuals access to complimentary credit monitoring. NOTE: annexed hereto as Exhibit A is a sample of the Notification sent to the individuals potentially impacted by the security incident. Please be advised that we are continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of ESHA's systems to help prevent this from happening in the future.

ESHA began mailing notification letters on November 15, 2024 to all individuals whose personal and/or protected health information may have been accessed and/or acquired in connection with the incident. Of these individuals, we are of the belief that two (2) individuals were New Hampshire residents. We anticipate that it will take five days for individuals to receive this letter. If an individual does not receive a letter, but would like to know if he or she was potentially affected by this incident, or if an individual has any questions or would like additional information, they may call ESHA's dedicated assistance line at 888-458-5630 between the hours of 9:00am to 9:00pm EST, Monday through Friday.

Should you have any questions or wish to further discuss, please do not hesitate to contact the undersigned.

Sincerely

Gregory N. Brescia

cc: Mark Ishman

EXHIBIT A

ESHA, INC.

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

ESHA, Inc ("**ESHA**") provides certain revenue cycle management services to <<Practice Name>> and understands the importance of protecting your information. ESHA is sending you this notice to inform you that it recently identified and addressed a security incident that may have involved your personal identifiable information and/or protected health information. This notice describes the incident, ESHA's investigation and the measures that we have taken in response to this incident. ESHA has obtained confirmation to the best of its ability that the files are no longer in the possession of third party(ies) associated with this incident, and it is entirely possible that any specific individual's personal information was *not impacted as a result* of the incident.

What Happened? On July 19, 2024, ESHA became aware of a data security incident involving suspicious activity in its network (the "**Security Incident**"). ESHA responded immediately by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. ESHA's immediate response enabled near seamless restoration of access to its systems and continuous operation of its services to its customers.

ESHA also simultaneously retained a forensic investigation firm to determine the nature of the Security Incident and identify any individuals whose information may have been compromised. The forensic investigation determined that first access to ESHA's network occurred on approximately July 13, 2024 through July 17, 2024. While the findings of the forensic investigation were not conclusive, a limited number of files may have been accessed or acquired in connection with the Security Incident. ESHA has obtained confirmation to the best of its ability that the files are no longer in the possession of third party(ies) associated with this incident, and it is entirely possible that any specific individual's personal information was *not impacted as a result* of the incident.

What Information Was Involved? In continuing its thorough investigation, ESHA undertook a comprehensive manual review process to review the entirety of the files that may have been accessed and/or acquired in connection with the Security Incident and identify the specific individuals with information contained therein.

In an abundance of caution, ESHA is providing this notification to you as your information was identified in the files that may have been accessed and/or acquired in connection with the incident. Specifically, the information identified in these files included <<Data Elements>>. **Please note that it is entirely possible that your specific information was not compromised as a result of the incident.**

What We Are Doing. As stated above, ESHA responded immediately to the Security Incident and undertook efforts by physically disconnecting all equipment and undertaking necessary efforts to restore its systems. ESHA retained a forensic investigation firm to thoroughly investigate the Security Incident and identify any individuals whose information may have been compromised. Please be advised that ESHA is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

FREE CREDIT MONITORING/INSURANCE: Additionally, we are offering you a free <<12/24>> Month membership to Equifax Credit Watch Gold credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. **This product also includes various features such as up to $1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. Equifax Credit Watch Gold is completely free to you** and enrolling in this program will not hurt your credit score. For more information on identity theft protection and Equifax Credit Watch Gold, including instructions on how to activate your complimentary <<12/24>> month membership, please see the additional information attached to this letter***. TO TAKE ADVANTAGE OF THE FREE CREDIT MONITORING OFFER, YOU MUST ENROLL BY <<ENROLLMENT DEADLINE>>.***

What You Can Do. We are aware of how important your personal information is to you. We encourage you to protect yourself from potential harm associated with this incident by enrolling in the credit monitoring service, closely monitoring all mail, email, or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements, explanation of benefits statements, and credit reports for unauthorized activity, and to report any such activity or any suspicious contact whatsoever to law enforcement if warranted.

For More Information. For further information on steps you can take to prevent against possible fraud or identity theft, please see the attachments to this letter. ESHA understands the importance of protecting your personal information, and deeply regrets any concern this may have caused to you. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 888-458-5630, Monday through Friday 9 AM to 9 PM Eastern.**

Sincerely,

Christian J. Hoffmann, III
CFO
ESHA, Inc

6913 CAMP BOWIE BLVD.* SUITE 171 * FORT WORTH, TEXAS 76116
(817) 731-6121 * (800) 704-2659 * FAX (817) 732-8015

EQUIFAX®

<Name 1>
Enter your Activation Code: <*ACTIVATION CODE*>
Enrollment Deadline: <**Enrollment Deadline**>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

6913 CAMP BOWIE BLVD.* SUITE 171 * FORT WORTH, TEXAS 76116
(817) 731-6121 * (800) 704-2659 * FAX (817) 732-8015