



July 25, 2023

Via electronic-mail: DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re:	Our Client	:	American Board of Internal Medicine
	Matter	:	Data Security Incident on May 31, 2023
	LBBS File #	:	16516.99

Dear Attorney General Formella:

We represent the American Board of Internal Medicine (“ABIM”) headquartered in Philadelphia, Pennsylvania, with respect to a potential data security incident described in more detail below. ABIM takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents that were potentially affected, what information has been compromised, and the steps that ABIM is taking in response to this incident. We have also enclosed hereto a sample of the notifications made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On or about May 31, 2023, ABIM was notified that its third-party vendor, Progress Software was impacted by a data security incident involving the MOVEit Transfer software vulnerability. As a result, an unauthorized third-party was able to access and download some of ABIM’s data. Affected individuals’ _____ to the extent such existed on the network, may have been compromised. Notably, the exposed data elements for each individual were different.

As of this report, ABIM has not received any reports of related identity theft since the date of the incident (May 31, 2023 to present).

2. New Hampshire Residents Notified

A total of and twenty-one (21) residents of New Hampshire were potentially affected by this security incident. A notification letter to these individuals will be mailed on July 25, 2023, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

This incident occurred within the MOVEit Transfer platform. Therefore, the actions available to ABIM were limited. However, ABIM takes the security of all data seriously. Given this, ABIM has taken steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in its systems. We have been working with law enforcement to help respond to this incident, along with cybersecurity experts to review all policies and procedures relating to the security of ABIM's systems and information life cycle management.

Although ABIM is not aware of any evidence of misuse of personal information, ABIM extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

ABIM 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

Very truly yours,

Lewis Brisbois Bisgaard & Smith, LLC

Tawana Johnson, Esq.

cc: Robert Walker, Esq.
(Lewis Brisbois LLC)

Enclosures: *Sample notification letter*



Return Mail to IDX
PO Box 480149
Niles, IL 60714

<FirstName> <LastName>
<Address1> <Address2>
<City>, <State><Zip>
<Country Name>

Via First-Class Mail

July 25, 2023

Notice of Data <<Breach/Incident>>

Dear Dr. <<Last Name>>,

The American Board of Internal Medicine (“ABIM”) is writing to inform you of a data security incident that may have exposed your personal information. We take the security of your personal information very seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On or about May 30, 2023, ABIM detected and stopped suspicious activity within its network environment. Upon detecting this incident, we moved quickly to secure our network environment and launched a thorough investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to our systems and any personal information.

After the comprehensive forensic investigation concluded, we discovered that your
, to the extent that such may have existed on the network, could have been exposed as a result of this incident.

As of this writing, ABIM has not received any reports of related identity theft since the date of the incident (May 30, 2023 to present).

What We Are Doing:

We take the security of all information very seriously. Given this, we have taken steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in our systems. We have been working with law enforcement to help respond to this incident, along with cybersecurity experts to review all policies and procedures relating to the security of ABIM’s systems and information life cycle management.

What You Can Do:

ABIM is providing you with identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: _____ of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling _____ or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is _____.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed hereto you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call _____

ABIM values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,

American Board of Internal Medicine

Additional Information

Credit Reports: 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.

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 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze
---	---	--

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 listed above.

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

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order 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 generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; 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 www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately [#] Rhode Island residents that may be impacted by this event.