MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

4843 Colleyville Blvd, Suite 251-388
Colleyville, TX 76034

May 26, 2020

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Pennsylvania Bar Association ("PBA") located at 5080 Ritter Rd., Mechanicsburg, PA 17055, and are writing to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PBA does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 7, 2020, the Pennsylvania Bar Association received notice that certain members discovered suspicious activity in their financial accounts. PBA's IT professionals immediately investigated the incident and discovered malicious code embedded in its website, which was removed on April 8, 2020; however, the PBA was informed of a similar incident on April 21, 2020. Although the forensic investigation is ongoing, we have determined that certain names and credit card information input into PBA's website may have been accessed by an unauthorized individual. Given the potential access to sensitive data, PBA has chosen to notify impacted and potentially impacted individuals of this incident and has provided all individuals notified with resources that can be used to protect their personal information.

Notice to New Hampshire Residents

On or about May 26, 2020, PBA provided written notice of this incident to all affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

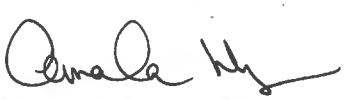
Upon discovering the event, PBA moved quickly to investigate and respond to the incident, assess the security of PBA systems, and notify potentially affected individuals. PBA is also reviewing its policies, procedures, and standards to ensure that PCI compliance is maintained.

Additionally, PBA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. PBA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1697.

Very truly yours,



Amanda Harvey of
MULLEN COUGHLIN LLC

Enclosure
ANH/wds

EXHIBIT A

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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

This correspondence is meant to inform you of an incident which may have exposed your personal information, including your name and credit card information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your data. This letter contains information about the incident and resources we are making available to you.

What happened?

On April 7, 2020, the Pennsylvania Bar Association ("PBA") received notice that certain customers discovered suspicious activity in their financial accounts on the Pennsylvania Bar Institute (PBI) website. PBA's IT professionals immediately investigated the incident and discovered malicious code in the environment, which was removed on April 8, 2020; however, the PBA was informed of a similar incident on April 21, 2020. Although the forensic investigation into the incident is ongoing, we have determined that your name and financial information were potentially compromised as a result of the incidents. Given the potential access to your data, we have chosen to notify you and provide you with resources that can be used to protect your personal data.

What we are doing.

Pennsylvania Bar Association values the security and confidentiality of customer information. To that end, in addition to engaging a vendor to conduct a forensic investigation to determine the scope of compromise and identify the vulnerability which allowed for the malicious script to be integrated into the PBI website, we have also notified the FBI, who has opened an investigation into this incident. Further, we have removed the malicious code from and applied security patches to the PBI website to mitigate the risk of further compromise. Finally, we are reviewing our technical policies and procedures and implementing best practices so as to prevent similar incidents in the future.

What you can do.

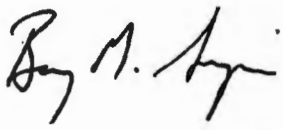
Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. Further, if you have not done so, we recommend calling your credit card company immediately and informing them of this incident and diligently monitoring your credit card statements and credit reports for suspicious transactions.

For more information.

If you have questions, please call 855-917-3503, Monday through Friday from 9 a.m. to 9:00 p.m. EST.

Protecting your information is important to us. We trust that the actions we are taking in response to this incident demonstrate our continued commitment to your security and satisfaction.

Sincerely,



Barry Simpson
Executive Director

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability 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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.