LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Ave., Suite 9000
Portland, OR 97204
Sean.Hoar@lewisbrisbois.com
Direct: 971-712-2795

December 18, 2020

VIA EMAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
E-Mail: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent the Washington State Bar Association ("WSBA"), located in Seattle, Washington. This letter is being sent on behalf of the WSBA because personal information belonging to Washington residents may have been affected by a recent data security incident. This information may have included unauthorized access to payment card information.

On November 12, 2020, the WSBA detected that the mywsba.org site appeared to contain unauthorized computer code. The site was immediately disabled and the WSBA began an investigation. It engaged a digital forensics firm to assist in determining whether personal information may have been acquired without authorization. On December 2, 2020, the investigation determined that payment card information of 4,051 Washington residents may have been affected. It appears that information pertaining to transactions between March 10 and November 12, 2020 may have been acquired without authorization.

The WSBA is in the process of notifying the Washington residents whose payment card information may have been affected. A sample copy of the notification letter sent to the affected individuals is included with this correspondence. The WSBA has also undertaken measures to enhance the security of the site, including extensive vulnerability testing, in an attempt to prevent similar events in the future. Should you have any questions or need additional information, please contact me at (971) 712-2795 or via email at Sean.Hoar@lewisbrisbois.com.

Sincerely,

Sean B. Hoar
Lewis Brisbois Bisgaard & Smith LLP

Enclosure: Sample Consumer Notification Letter

1325 Fourth Avenue, Suite 600
Seattle, Washington 98101-2539

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident that involved your personal information. The Washington State Bar Association ("WSBA") takes the privacy and security of your information very seriously, which is why we are informing you of the incident and providing information about steps you can take to protect your information.

What Happened. On November 12, 2020, the WSBA detected that the mywsba.org site appeared to contain unauthorized computer code. We immediately disabled the site and began an investigation. We also engaged a digital forensics firm to assist in determining whether personal information may have been acquired without authorization. On December 2, 2020 the investigation determined that your payment card information may have been affected. It appears that information pertaining to transactions between March 10 and November 12, 2020 may have been acquired without authorization.

What Information Was Involved. The information included your payment card(s) with the following last four digits: <<b2b_text_1(VariableDataElements)>>.

What We Are Doing. In addition to steps described above, we have taken measures to enhance the security of the site. We also reported the matter to the Federal Bureau of Investigation, and will provide whatever cooperation may be necessary to hold the perpetrators accountable. On the following page, we have also provided steps you can take to protect your personal information.

What You Can Do. You can follow the recommendations on the following page to protect your personal information. One of the recommendations is that you contact the financial institution or company with which the payment card account is maintained, and assess whether it is appropriate to replace the card.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-???-???-???? from 6:00 a.m. to 3:30 p.m. Pacific, Monday through Friday, excluding major U.S. holidays. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Terra Nevitt
Interim Executive Director

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: We recommend that you contact the financial institution or company with which the affected payment card account is maintained, and assess whether it is appropriate to replace the card. We also recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: Although the unauthorized acquisition of payment card information is not likely to have any effect on a credit file, as a proactive measure you may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
ifraud@ag.ny.gov	1-888-743-0023	1-877-566-7226	401-274-4400
1-212-416-8433			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf