RECEIVED
JUL 01 2020
CONSUMER PROTECTION

BakerHostetler

Baker&Hostetler LLP
45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Gerald J. Ferguson
direct dial: 212.589.4238
gferguson@bakerlaw.com

June 30, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, The New York City Bar Association and the City Bar Fund (collectively "the City Bar"), to notify you of a data security incident involving one of its third-party vendors, Advanced Solutions International ("ASI").

ASI is the developer of the iMIS software, a member management and e-commerce platform that the City Bar uses on its website, www.nycbar.org. On April 30, 2020, the City Bar was alerted to suspicious activity that involved its website's e-commerce portal. Upon learning of this, the City Bar removed the unauthorized code from the iMIS platform hosted on its web server and launched an investigation with the assistance of a leading cybersecurity firm.

Through this investigation, completed on May 20, 2020, the City Bar identified unauthorized code designed to capture cardholder data had been inserted in the web server that hosts the iMIS e-commerce platform on its website. The unauthorized code was present on the City Bar's website between April 23, 2020 and May 1, 2020, during which time it could have captured cardholder data submitted by consumers who placed orders or made donations following completion of the checkout process.

The investigation concluded that the unauthorized code was capable of potentially capturing cardholder names, billing and shipping addresses, email addresses, telephone numbers, payment card numbers, expiration dates, and card security codes (CVV).

Beginning on June 30, 2020, the City Bar will mail a notification letter via United States Postal Service First-Class mail to one New Hampshire resident whose cardholder data may have been involved in this incident, in accordance with N.H. Rev. Stat. Ann. § 359-C:20.[1] A copy of the notification letter is enclosed.

[1] This does not waive the City Bar's objection that New Hampshire lacks personal jurisdiction over it regarding any claims relating to this incident.

To help prevent a similar incident from occurring in the future, the City Bar has and implemented advanced malware protection software with enhanced monitoring and alerting capabilities.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Gerald J. Ferguson

Enclosure

NEW YORK CITY BAR

Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

[redacted]

June 30, 2020

Dear [redacted]

The New York City Bar Association and the City Bar Fund (collectively "the City Bar"), are committed to protecting the confidentiality and security of the information we maintain. We are writing to inform you about an incident involving one of our third-party vendors, Advanced Solutions International ("ASI"), that may have involved some of your information. This notice explains the incident, measures that have been taken, and some steps you can take in response.

ASI is the developer of the iMIS software, a member management and e-commerce platform that the City Bar uses on our website, www.nycbar.org. On April 30, 2020, the City Bar was alerted to suspicious activity that involved our website's e-commerce site. Upon learning of this, the City Bar immediately removed the unauthorized code from the iMIS platform hosted on our web server and launched an investigation with the assistance of a leading cybersecurity firm.

Through this investigation, completed on May 20, 2020, the City Bar identified unauthorized code designed to capture cardholder data had been inserted in the web server that hosts the iMIS e-commerce platform on our website. The unauthorized code was present on the City Bar's website between the dates of April 23, 2020 and May 1, 2020.

During this time period, the unauthorized code could have captured cardholder data entered during the checkout process by customers who placed orders or made donations on the City Bar's website. Our investigation concluded that the unauthorized code was capable of potentially capturing cardholder names, billing and shipping addresses, email addresses, telephone numbers, payment card numbers, expiration dates, and card security codes (CVV). We are notifying you because you placed an order or made a donation on the City Bar's website during this period.

It is always advisable to review your payment card statements for any unauthorized charges. You should immediately report any such charges to your card issuer because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. The phone number to call is usually on the back of your payment card. Information on additional steps you can take can be found on the following pages.

We regret any concern or inconvenience this causes you. To help prevent a similar incident from occurring in the future, the City Bar has implemented advanced malware protection software with enhanced monitoring and alerting capabilities. If you have questions, please call 866-279-5170, Monday – Friday, from 9:00 a.m. until 7:00 p.m., Eastern Time.

Sincerely,

Bret Parker
Executive Director

NYBAR-IND-GEN

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106,
1-860-808-5318, www.ct.gov/ag

District of Columbia: The New York City Bar Association's mailing address is 42 W 44th Street, New York, NY 10036. You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: The New York City Bar Association's mailing address is 42 W 44th Street, New York, NY 10036. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.