



Elizabeth R. Dill
550 E. Swedesford Road, Suite 270
Wayne, PA 19087
Elizabeth.Dill@lewisbrisbois.com
Direct: 215.977.4101

January 9, 2021

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent AHIMA: American Health Information Management Association (“AHIMA”) located in Chicago, IL. We are writing pursuant to N.H. Rev. Stat. §§ 359-C:19 - C:21 because AHIMA has learned of a data security incident that may have affected the personal information of 39 New Hampshire residents. The information that was involved in the incident includes names, payment card numbers, expiration dates, and security codes.

AHIMA maintains an online store (<https://my.ahima.org/store/>), through which customers can make purchases and register for courses. Upon learning of potential suspicious activity occurring in the online store, AHIMA took immediate steps to secure its system, and conducted an internal investigation. AHIMA also worked with a leading digital forensics firm to determine what happened as well as whether the payment card information of AHIMA’s customers had been affected. On December 3, 2020, AHIMA’s investigation determined that the incident involved the payment card information of AHIMA customers who made purchases through the online store between June 26, 2020 and July 29, 2020 and between October 1, 2020 and October 16, 2020. On December 28, 2020, AHIMA confirmed that the affected individuals include 39 residents of New Hampshire.

AHIMA has reported the incident to the Federal Bureau of Investigation in order to protect its customers’ payment card information and prevent fraudulent activity. Notification letters to the affected individuals were mailed on January 5, 2021. A sample copy of the letter that was mailed to the New Hampshire residents is attached hereto. As referenced in the letter, AHIMA is providing the individuals with 12 months of complimentary identity protection services through ID Experts.

Please do not hesitate to contact me should you have any questions. Thank you.

Sincerely,

A handwritten signature in purple ink that reads "Elizabeth R. Dill". The signature is written in a cursive style with a distinct dot over the 'i' in "Dill".

Elizabeth R. Dill of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Consumer notification letter



C/O IDX
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 5, 2021

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

The American Health Information Management Association (AHIMA) is writing to notify you of a data security incident relating to your purchase through our online store (<https://my.ahima.org/store/>) that may have involved your payment card information. At AHIMA, we take the privacy and security of your information very seriously. I want to inform you of the incident and to advise you about certain steps you can take to ensure your information is protected.

What happened?

On October 13, 2020, we learned of suspicious activity relating to our online store. Upon discovering the activity, we took immediate steps to secure our system and customer information. We also immediately began an investigation into the incident. In connection with that investigation, AHIMA engaged a nationally recognized digital forensics firm to determine whether any customer information had been accessed or acquired without authorization. On December 3, 2020, the investigation determined that certain payment card information may have been exposed as a result of the incident.

What Information Was Involved?

The incident affected certain payment card information belonging to individuals who made purchases through our online store between July 26, 2020 and July 29, 2020 and October 1, 2020 and October 16, 2020. The payment card information that may have been compromised included names, card numbers, expiration dates, and security codes.

What We Are Doing:

As soon as we discovered the incident, we took the steps described above. We have also reported the incident to the Federal Bureau of Investigation and will cooperate with them to hold the perpetrators accountable.

In addition, we are offering you complimentary identity theft protection services through IDX. Your IDX identity protection membership includes 12 months of fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised due to this incident.

What You Can Do:

You should **follow the recommendations included with this letter** to ensure that your personal information is protected, including reviewing your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the card immediately.

We encourage you to contact our dedicated call center for more information by calling 833-754-1797. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. IDX has been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

There is no need to enroll in your IDX identity theft recovery services – you are automatically covered. If you have questions or concerns about possible fraud, please contact IDX for assistance.

For More Information:

Enclosed is a document that provides additional details regarding protection of your information. You may also contact 833-754-1797 regarding any additional questions you may have.

On behalf of AHIMA, I want to assure you that we take this matter very seriously. We value our members and customers, and we apologize for any concern or inconvenience this matter may cause you. Thank you for your support.

Sincerely,

A handwritten signature in cursive script that reads "Amy A Mosser".

Amy A Mosser, COO
American Health Information Management Association (AHIMA)
233 N. Michigan Avenue, 21st Floor
Chicago, IL 60601 - 50809

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, I recommend that you remain vigilant by reviewing 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 also should 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 (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 print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

Fraud Alert: 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 at least 90 days. 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 federal 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. You cannot be charged to place, lift or remove a security freeze.

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

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights under the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf