EXHIBIT 1

We represent CPR AED Course LLC dba American Health Care Academy ("AHCA"), located at P.O. Box 154927 Irving, Texas 75015. AHCA writes to notify your office of an incident that may impact the privacy of personal information relating to one hundred forty-five (145) Maine residents. AHCA reserves the right to supplement this notice with new significant facts learned subsequent to its submission. By providing this notice, AHCA does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 29, 2020, AHCA was alerted to unusual activity related to certain of its customers' payment cards. AHCA immediately commenced an investigation, working with third party forensic investigators, to assess the nature and scope of the activity. The investigation determined the existence of a webshell with the capability of accessing information stored in AHCA's environment. While the investigation could not confirm whether personal information was compromised as a result of this incident, this possibility could not be ruled out. Therefore, in an abundance of caution, AHCA undertook a comprehensive review of the information residing in its database to confirm the types of information within the database and the individuals to whom the information related. This review was completed on January 15, 2021.

The investigation determined that first and last names, as well as debt or credit card information, related to Maine residents may have been accessible within AHCA's database.

Notice to Maine Residents

On March 15, 2021, AHCA provided written notice of this incident to potentially affected individuals. This includes approximately one hundred forty-five (145) Maine residents whose personal information under state law may have been accessible. Written notice to the individuals is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of this incident, AHCA moved quickly to assess the security of its database and systems, reset relevant passwords, and to notify potentially impacted individuals. At the time of the incident AHCA stored customer payment card information in its database for approximately 24 hours after a transaction for quality assurance purposes. However, as of December 16, 2020, AHCA no longer temporarily stores any payment card information.

In its notice letters, AHCA is providing affected individuals with guidance on how to better protect themselves against identity theft and fraud. This guidance includes information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant about incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, the respective state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. AHCA will also be providing notice of this event to other regulators as may be required under applicable state law.

EXHIBIT A

<<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 Possible Data Breach Relating to Your Information

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

CPR AED Course LLC dba American Health Care Academy ("AHCA") writes to make you aware of a recent incident involving your personal information. This letter provides information about the incident, our response, and resources available to you to help protect your information from potential misuse, should you feel it necessary to do so.

What Happened? On November 29, 2020, we were alerted to unusual activity related to certain of our customers' payment cards. We immediately commenced an investigation, working with third party forensic investigators, to assess the nature and scope of the activity. The investigation determined the existence of a webshell with the capability of accessing information stored in our environment. While the investigation could not confirm whether personal information was compromised as a result of this incident, this possibility could not be ruled out. Therefore, in an abundance of caution, we undertook a comprehensive review of the information residing in our database to confirm the types of information within the database and the individuals to whom the information related. This review was completed on January 15, 2021, and we determined that certain of your personal information was stored within the impacted account.

What Information Was Involved? Our investigation determined that your first and last name, as well as your debit or credit card number, temporarily resided in the potentially impacted database. At the time of the incident AHCA stored customer payment card information in our database for approximately 24 hours after a transaction for quality assurance purposes. However, as of December 16, 2020, we no longer temporarily store any payment card information.

What We Are Doing. We take the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to assess the security of our database and systems, reset relevant passwords, and to notify potentially impacted individuals. As part of our ongoing commitment to information security, we have already enhanced existing policies and procedures, including changes to our payment card collection process where we no longer store any payment card information. Additionally, we are notifying potentially impacted individuals, including you, so that you may take further steps to protect your information, should you feel it appropriate to do so.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For More Information. We recognize you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-956-1061, Monday – Friday, 8:00 a.m. to 5:30 p.m. Central Time (excluding U.S. national holidays). You may also write to AHCA at: P.O. Box 154927 · Irving, Texas 75015.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is important to us, and AHCA remains committed to safeguarding information in our care.

Sincerely,

Shay Lakhani
Manager
American Health Care Academy

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the 3 major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the 3 major credit bureaus listed below directly to request a free copy of your credit report. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-alerts

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

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); and 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the Office of the District of Columbia Attorney General can be contacted at: 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov; or you may visit the website of the Office of the District of Columbia Attorney General at https://oag.dc.gov/.

For Kentucky residents, the Office of the Attorney General of Kentucky can be contacted at, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601; www.ag.ky.gov; or 1-502-696-5300.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or 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 to Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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; or https://ag.ny.gov.

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

Oregon residents, the Oregon Department of Justice can be contacted at: 1162 Court Street NE, Salem, OR 97301-4096; www.doj.state.or.us/; or 1-877-877-9392.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 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 X Rhode Island resident(s) impacted by this incident.