

[DATE]

<<First Name>><<Last Name>>
<<Address_Line_1>>
<<Address_Line_2>>
<<City>><<State>><<Zip>>

RE: Notice of Data Breach

Dear <<First Name>><<Last Name>>:

Health Fitness Corporation (“HealthFitness”) is a <<Client_Def2>> vendor that provides wellness services to <<Client_Def2>> participants. <<Client_Def4>> HealthFitness is writing to inform you of a recent data security incident that may impact your personal information. We sincerely apologize and we take the security of your personal information very seriously. We are providing this notice to you so you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so.

What Happened? On June 27, 2018, HealthFitness discovered that certain records relating to health coaching, specifically physician consent forms, participant liability waivers, and certain health coaching session audio files, were being stored on a server that was inadvertently searchable on the Internet due to a software misconfiguration. By way of background, the physician consent forms and participant liability waivers were required of certain participants prior to participating in a physical activity in our health coaching program.

HealthFitness found evidence that these files were accessed by web crawlers, at least as early as August of 2015. Web crawlers are often used by search engines, such as Bing or Google, to index web pages. Most of these files were scanned documents and many contained handwritten information, which is not easily recognizable by web crawlers and search engines.

This exposure was discovered during an internal web application security test by HealthFitness. Access to the records was immediately removed, and HealthFitness began an investigation using both internal resources and third-party forensic investigators.

As the exposed files contained handwritten information and audio files, significant resources were needed to determine the contents of the records and the identities of the potentially impacted individuals to whom the documents related. The forensics firm engaged by HealthFitness provided a report containing the contents of these files on July 20, 2018, at which point we discovered that your information was impacted. HealthFitness notified <<Client_Def2>> on <<Client_Def3>> of this incident.

What Information Was Involved? We have determined that the accessible files included the name of your employer, as well as your <<Client_Def1>> .

What We Are Doing. We take this incident, and information security, very seriously at HealthFitness. We continue to diligently investigate and assess this incident. We have addressed the software misconfiguration that caused this, and are currently taking steps to further enhance the security of our systems to better protect against future incidents of this kind. In addition to providing this notice, we are providing complimentary access to 12 months of credit monitoring and identity restoration services with AllClear ID, as well as information on what you can do to better protect against the possibility of identity theft and fraud.

What You Can Do. As an added precaution, we have arranged to have AllClear ID protect your identity for «Time» months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next «Time» months.

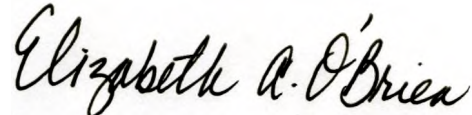
AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling «DID_Phone» using the following redemption code: {RedemptionCode}.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

For More Information. We sincerely regret any concern this incident may cause you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call XXX, Monday through Friday, 8:00 a.m. to 6:00 p.m. E.S.T (excluding U.S. holidays).

Sincerely,



Elizabeth O'Brien
Chief Privacy Officer

Steps You Can Take to Protect Against Identity Theft and Fraud

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 three 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 three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call
1-800-349-9960)
<https://www.freeze.equifax.com>

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

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/credit-freeze

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at <https://www.irs.gov/Individuals/Identity-Protection> for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> for more information.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission’s fraud website is www.identitytheft.gov.

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); 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); 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. A guest can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement. **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 violator. 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 Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **For Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401)247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. This notice has not been delayed as a result of a law enforcement investigation.