RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement ("Agreement") are:

A. The United States Department of Health and Human Services, Office for Civil Rights ("HHS"), which enforces the Federal standards that govern the privacy of individually identifiable health information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule"), the Federal standards that govern the security of electronic individually identifiable health information (45 C.F.R. Part 160 and Subparts A and C of Part 164, the "Security Rule"), and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the "Breach Notification Rule"). HHS has the authority to conduct compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules (the "HIPAA Rules") by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).

B. Health Fitness Corporation ("Health Fitness") is a business associate as defined at 45 C.F.R. § 160.103 and is therefore required to comply with the HIPAA Rules. Health Fitness is headquartered in Lake Forest, Illinois and provides wellness plans to clients across the United States. Health Fitness is one of several subsidiaries that was acquired, and that is now owned and managed by the Trustmark Mutual Holding Company.

HHS and Health Fitness shall together be referred to herein as the "Parties."

2. Factual Background and Covered Conduct.

Health Fitness reported to OCR that beginning approximately in August 2015, electronic protected health information ("ePHI") became discoverable on the internet and was exposed to automated search devices (web crawlers) resulting from a software misconfiguration on the server housing the ePHI. Health Fitness discovered the breach on June 27, 2018.

In the course of investigating this breach, OCR determined that the following conduct occurred ("Covered Conduct"):

A. Health Fitness failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI that it holds until January 19, 2024. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

3. No Admission. This Agreement is not an admission of liability by Health Fitness.

4. No Concession. This Agreement is not a concession by HHS that Health Fitness is not in violation of the HIPAA Rules and not liable for civil money penalties.

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Numbers: 19-320289, 19-320294, 19-321694, and 19-330860 and any violations of the HIPAA Rules related to the Covered Conduct specified in paragraph I.2 of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden, and expense of formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and Health Fitness has agreed to pay HHS, the amount of **$227,816** ("Resolution Amount"). Health Fitness agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in paragraph II.14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. Health Fitness has entered into and agrees to comply with the Corrective Action Plan ("CAP"), attached as Appendix A, which is incorporated into this Agreement by reference. If Health Fitness breaches the CAP and fails to cure the breach as set forth in the CAP, then Health Fitness will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon Health Fitness's performance of its obligations under this Agreement, HHS releases Health Fitness from any actions it may have against Health Fitness under the HIPAA Rules arising out of or related to the Covered Conduct identified in paragraph I.2 of this Agreement. HHS does not release Health Fitness from, nor waive any rights, obligations, or causes of action other than those arising out of or related to the Covered Conduct and referred to in this paragraph. This release does not extend to actions that may be brought under section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

9. Agreement by Released Parties. Health Fitness shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. Health Fitness waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a- 7a) and 45 C.F.R. Part 160 Subpart E, and HHS claims collection regulations at 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. Binding on Successors. This Agreement is binding on Health Fitness and its successors, heirs, transferees, and assigns.

11. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

12. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against or by any other person or entity.

13. Effect of Agreement. This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement shall be set forth in writing and signed by all Parties.

14. Execution of Agreement and Effective Date. The Agreement shall become effective (*i.e.*, final and binding) upon the date of signing of this Agreement and the CAP by the last signatory (Effective Date).

15. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a civil money penalty ("CMP") must be imposed within six years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of this Agreement, Health Fitness agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of Health Fitness's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the violations which are the subject of this Agreement. Health Fitness waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the covered conduct identified in paragraph I.2 that is filed by HHS within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

16. Disclosure. HHS places no restriction on the publication of the Agreement. In addition, HHS may be required to disclose material related to this Agreement to any person upon request consistent with the applicable provisions of the Freedom of Information Act, 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5.

17. Execution in Counterparts. This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

18. Authorizations. The individual(s) signing this Agreement on behalf of Health Fitness represent and warrant that they are authorized by Health Fitness to execute this Agreement. The individual(s) signing this Agreement on behalf of HHS represent and warrant that they are signing this Agreement in their official capacities and that they are authorized to execute this Agreement.

For Health Fitness Corporation

/s/ 12/20/2024

_____ _____

Date

Sean McManamy, SVP and President
Health Fitness Corporation

For U.S. Department of Health and Human Services

/s/ 12/20/2024

_____ _____

Andrea Oliver, Regional Manager
Office for Civil Rights

Date

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

HEALTH FITNESS CORPORATION

I. Preamble

Health Fitness Corporation (hereinafter known as "Health Fitness" hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS"). Contemporaneously with this CAP, Health Fitness is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. Health Fitness enters into this CAP as part of consideration for the release set forth in paragraph II.8 of the Agreement. Capitalized terms without definition in this CAP shall have the same meaning assigned to them under the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

Health Fitness has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Katie Licup
Vice President, Chief Compliance Officer
Trustmark
400 Field Drive
Lake Forest, IL 60045
klicup@trustmarkbenefits.com
Phone: (847) 283-3478

HHS has identified the following individual as its authorized representative and contact person with whom Health Fitness is to report information regarding the implementation of this CAP:

Andrea Oliver, Regional Manager
Office for Civil Rights, Rocky Mountain Region
Department of Health and Human Services
andrea.oliver@hhs.gov

Health Fitness and HHS agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions. Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including email, certified mail, overnight mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Effective Date and Term of CAP

The Effective Date for this CAP shall be calculated in accordance with paragraph II.14 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by Health Fitness under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date unless HHS has notified Health Fitness under section VIII hereof of its determination that Health Fitness breached this CAP. In the event of such a notification by HHS under section VIII hereof, the Compliance Term shall not end until HHS notifies Health Fitness that it has determined that the breach has been cured. After the Compliance Term ends, Health Fitness shall still be obligated to submit the final Annual Report as required by section VI and comply with the document retention requirement in section VII. Nothing in this CAP is intended to eliminate or modify Health Fitness's obligation to comply with the document retention requirements in 45 C.F.R. §§ 164.316(b) and 164.530(j).

IV. Time

In computing any period of time prescribed or allowed by this CAP, all days referred to shall be calendar days. The day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day which is not one of the aforementioned days.

V. Corrective Action Obligations

Health Fitness agrees to the following:

A. Annually Update Risk Analysis

1. Health Fitness shall review and update as necessary its Risk Analysis annually and submit the same to OCR within thirty (30) days of completion. As used herein, "Risk Analysis" means the identification and implementation of safeguards that comply with and carry out the standards and implementation specifications contained in the Security Rule. Health Fitness shall also promptly update the Risk Analysis in response to environmental or operational changes affecting the security of ePHI and submit the results to OCR within thirty (30) days of completion. Following an update to the risk analysis, Health Fitness shall assess whether its

existing security measures are sufficient to protect its electronic PHI, and revise its risk management plan, policies and procedures, and training materials, as needed.

B. Develop and Implement a Risk Management Plan

1. Health Fitness shall develop a risk management plan sufficient to address and mitigate any security risks and vulnerabilities identified in its Risk Analysis described in section V.A. above ("Risk Management Plan"). The Risk Management Plan shall include a process and timeline for Health Fitness's implementation, evaluation, and revision of their risk remediation activities.

2. The Risk Management Plan shall be forwarded to HHS for review and approval within one hundred twenty (120) days of the Effective Date. HHS shall approve, or, if necessary, require revisions to Health Fitness's Risk Management Plan.

3. Upon receiving HHS's notice of required revisions, if any, Health Fitness shall have thirty (30) days to revise the Risk Management Plan accordingly and forward to HHS for review and approval. This process shall continue until HHS approves the Risk Management Plan.

4. Within thirty (30) days of HHS's approval of the Risk Management Plan, Health Fitness shall finalize and officially adopt the Risk Management Plan in accordance with its applicable administrative procedures.

C. Implement Process for Evaluating Environmental and Operational Changes

Within one hundred twenty (120) days of the Effective Date, Health Fitness shall develop a process to evaluate any environmental or operational changes that affect the security of Health Fitness's ePHI. HHS shall review and recommend changes to the process. Upon receiving HHS' recommended changes, Health Fitness shall have sixty (60) days to provide a revised process to HHS for review and approval. Health Fitness shall implement its process, including distributing to workforce members with responsibility for performing such evaluations within ninety (90) days of HHS' approval.

D. Policies and Procedures

1. Health Fitness shall develop, maintain, and revise, as necessary, its written policies and procedures ("Policies and Procedures") to comply with the Federal standards that govern the privacy and security of individually identifiable health information and to address any threats and vulnerabilities to the ePHI identified in the risk analysis and risk management plan required by Sections V.A and V.B.

2. Within one hundred (120) days of HHS's approval of the Risk Management Plan identified in Section V.B., Health Fitness shall provide such Policies and Procedures, consistent with paragraph 1 above, to HHS for review and approval. Upon receiving any required changes to such Policies and Procedures from HHS, Health Fitness shall have thirty (30) days to revise the Policies and Procedures accordingly and provide the revised Policies and Procedures to HHS for

review and approval. This process shall continue until HHS approves such Policies and Procedures.

E. Minimum Content of the Policies and Procedures

The Policies and Procedures required by Paragraph V.D above shall include, but not be limited to, the following provisions, standards, implementation specifications and obligations:

Privacy Rule Provisions:

1. Uses and Disclosures of PHI - 45 C.F.R. § 164.502(a)

Security Rule Provisions:

2. Administrative Safeguards, including all required and addressable implementation specifications – 45 C.F.R. § 164.308(a) and (b).
3. Physical Safeguards, including all required and addressable implementation specifications – 45 C.F.R. § 164.310.
4. Technical Safeguards, including all required and addressable implementation specifications – 45 C.F.R. § 164.312.
5. Policies and Procedures and documentation requirements. – 45 C.F.R. § 164.316.

Breach Notification Rule Provisions:

1. Notification by a business associate, including all required and addressable implementation specifications – 45 C.F.R. §164.410.

F. Distribution and Updating of Policies and Procedures

1. Health Fitness shall distribute the Policies and Procedures identified in Section V.D., (a) to all members of the workforce whose job responsibilities involve the handling of ePHI within thirty (30) days of HHS's approval of such Policies and Procedures, and (b) to new members of the workforce whose job responsibilities involve the handling of ePHI within thirty (30) days of the beginning of service.

2. Health Fitness shall require, at the time of distribution of the Policies and Procedures, a signed written or electronic certification from all members of the workforce whose job responsibilities involve the handling of ePHI, stating that the workforce members have read, understand, and shall abide by such Policies and Procedures.

3. Health Fitness shall assess, update, and revise, as necessary, the Policies and Procedures at least annually. Health Fitness shall provide any revised Policies and Procedures to HHS for review and approval. Within 30 days of the effective date of any approved substantive revisions by HHS, Health Fitness shall distribute such revised Policies and Procedures to all members of its workforce whose job responsibilities involve the handling of ePHI and shall require new compliance certifications.

4. Health Fitness shall not provide any member of its workforce with access to PHI if that workforce member has not signed or provided the written or electronic certification required by paragraphs 2 and 3 of this section.

G. Reportable Events.

1. During the Compliance Term, Health Fitness shall, upon learning that a workforce member likely failed to comply with its Policies and Procedures described in Section V.D.1, promptly investigate this matter. If Health Fitness, after review and investigation, determines that a member of its workforce has failed to comply with its Policies and Procedures, Health Fitness shall report such events to HHS as provided in Section VI.B.2. Such violations shall be known as Reportable Events. The report to HHS shall include the following:

a. A complete description of the event, including the relevant facts, the persons involved, and the applicable provision(s) of Health Fitness's Privacy, Security, and Breach Notification policies and procedures; and

b. A description of the actions taken and any further steps Health Fitness plans to take to address the matter, to mitigate any harm, and to prevent it from recurring, including application of any appropriate sanctions against workforce members who failed to comply with its Privacy, Security, and Breach Notification policies and procedures.

2. If no Reportable Events occur during the Compliance Term, Health Fitness shall so inform HHS in the Implementation Report as specified in Section VI below.

VI. Implementation Report and Annual Reports

A. Implementation Report. Within 120 days after the receipt of HHS' approval of the Policies and Procedures required by section V.D.1, Health Fitness shall submit a written report to HHS summarizing the status of its implementation of the requirements of this CAP. This report, known as the "Implementation Report," shall include:

1. An attestation signed by an owner or officer of Health Fitness attesting that the Policies and Procedures are being implemented, have been distributed to all appropriate members of the workforce, and that Health Fitness has obtained all of the certifications required by sections V.F.;

2. An attestation signed by an owner or officer of Health Fitness listing all Health Fitness locations (including locations and mailing addresses), the corresponding name under which each location is doing business, the corresponding phone numbers and fax numbers, and an attestation that each location has complied with the obligations of this CAP; and

3. An attestation signed by an owner or officer of Health Fitness stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

B. Annual Reports. The one-year period beginning on the Effective Date and each subsequent one-year period during the course of the period of compliance obligations shall be referred to as "the Reporting Periods." Health Fitness also shall submit to HHS Annual Reports with respect to the status of and findings regarding Health Fitness's compliance with this CAP for each of the two (2) Reporting Periods. Health Fitness shall submit each Annual Report to HHS no later than 60 days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. An attestation signed by an owner or officer of Health Fitness attesting that the Policies and Procedures required by Section V of this CAP: (a) have been adopted; (b) are being implemented; and (c) have been distributed to all workforce members whose job responsibilities involve the handling of ePHI;

2. A summary of Reportable Events (defined in section V.G.1. identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events;

3. An attestation signed by an owner or officer of Health Fitness attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

Health Fitness shall maintain for inspection and copying, and shall provide to OCR, upon request, all documents and records relating to compliance with this CAP for six (6) years from the Effective Date.

VIII. Breach Provisions

Health Fitness is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions. Health Fitness may, in advance of any due date set forth in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A "timely written request" is defined as a request in writing received by HHS at least five (5) days prior to the date such an act is required or due to be performed.

B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty. The parties agree that a breach of this CAP by Health Fitness constitutes a breach of the Agreement. Upon a determination by HHS that Health Fitness has breached this CAP, HHS may notify Health Fitness of: (1) Health Fitness's breach; and (2) HHS' intent to impose a civil money penalty ("CMP") pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct set forth in paragraph I.2 of the Agreement and any other conduct that constitutes a violation of the HIPAA Privacy, Security, or Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

C. Health Fitness's Response. Health Fitness shall have 30 days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. Health Fitness is in compliance with the obligations of the CAP that HHS cited as the basis for the breach;
2. The alleged breach has been cured; or
3. The alleged breach cannot be cured within the 30-day period but that:

   (a) Health Fitness has begun to take action to cure the breach; (b) Health Fitness is pursuing such action with due diligence; and (c) Health Fitness has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period (or longer period that HHS agrees to pursuant to section VIII.C.3), Health Fitness fails to meet the requirements of this CAP to HHS's satisfaction, HHS may proceed with the imposition of a CMP against Health Fitness pursuant to 45 C.F.R. Part 160 for any violations of the Covered Conduct set forth in paragraph I.2 of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify Health Fitness in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

For Health Fitness Corporation

/s/ 12/20/2024

_____ _____

Date

Sean McManamy, SVP and President
Health Fitness Corporation

For United States Department of Health and Human Services

/s/ 12/20/2024

_____ _____

Andrea Oliver, Regional Manager
Office for Civil Rights

Date