# 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. Spencer Gifts LLC Flexible Benefits and Welfare Benefit Plans (The Plan) is a covered entity, as defined at 45 C.F.R. § 160.103, and is an employer sponsored group health plan. The Plan is sponsored and administrated by Spencer Gifts LLC (Spencer Gifts). The Plan provides certain health insurance benefits to eligible Spencer Gifts' employees and dependents.

HHS and The Plan shall together be referred to herein as the "Parties."

2. Factual Background and Covered Conduct.

On January 24, 2022, The Plan submitted a breach report to OCR stating that on November 25, 2021, Spencer Gifts began receiving complaints from employees that they were unable to connect to Spencer Gifts' virtual private network. The Plan learned the incident was due to a ransomware attack. The electronic protected health information (ePHI) of 10,023 individuals was affected by this breach, including names, addresses, zip codes, phone numbers, email addresses, and Social Security numbers.

HHS' investigation indicated that the following conduct occurred ("Covered Conduct"):

(i) The Plan failed to conduct an accurate and thorough risk analysis that assesses the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Plan's ePHI. *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).

(ii) The Plan failed to implement compliant HIPAA Privacy, Security, and Breach Notification Rule policies or procedures until after the breach. *See* 45 C.F.R. § 164.316(a); 45 C.F.R. § 164.530(i)(1).

3. No Admission. This Agreement is not an admission of liability by The Plan.

4. No Concession. This Agreement is not a concession by HHS that The Plan is not in violation of the HIPAA Rules and not liable for civil money penalties **("CMP").**

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Number 22-465057 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in paragraph 1.2 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. The Plan has agreed to pay HHS the amount of **$450,000** ("Resolution Amount"). The Plan agrees to pay the Resolution Amount in one-lump sum within seven (7) days of the Effective Date of this Agreement as defined in paragraph 11.14 pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. The Plan 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 The Plan breaches the CAP and fails to cure the breach as set forth in the CAP, then The Plan will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph 11.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon The Plan's performance of its obligations under this Agreement, HHS releases The Plan from any actions it may have against The Plan 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 The Plan 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. The Plan 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. The Plan 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 The Plan 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)(l), 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, The Plan agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of The Plan'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. The Plan 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.

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 The Plan represent and warrant that they are authorized by The Plan 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 Covered Entity**

/s/ 05/07/2026

Kevin Mahoney
Senior Vice President
Spencer Gifts LLC
Flexible Benefits and Welfare Benefit Plans

Date

**For U.S. Department of Health and Human Services**

/s/ 05/20/2026

Barbara Stampul
Regional Manager
Enforcement Division
Office for Civil Rights

Date

**Appendix A**

**CORRECTIVE ACTION PLAN**

**BETWEEN THE**

**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**AND**

**SPENCER GIFTS LLC Flexible Benefits and Welfare Benefit Plans**

## I. Preamble

Spencer Gifts LLC Flexible Benefits and Welfare Benefit Plans (hereinafter known as "The Plan") 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, The Plan is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. The Plan enters into this CAP as part of consideration for the release set forth in paragraph II.8 of the Agreement.

## II. Contact Persons and Submissions

### A. Contact Persons

The Plan 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:

Kevin Mahoney
Senior Vice President
Spencer Gifts LLC

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

Barbara Stampul
Regional Manager
Enforcement Division
Office for Civil Rights
U.S. Department of Health and Human Services
Sam Nunn Atlanta Federal Center, Suite 16T70
61 Forsyth Street, S.W.
Atlanta, GA 30303-8909

The Plan and HHS agreed 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 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 The Plan 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 The Plan under Section VIII hereof of its determination that The Plan 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 The Plan that it has determined that the breach has been cured. After the Compliance Term ends, The Plan 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 The Plan' 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

The Plan agrees to take the corrective action steps specified below.

A. Conduct Risk Analysis

1. The Plan shall conduct an accurate and thorough assessment of the potential security risks and vulnerabilities to the confidentiality, integrity, and availability of The Plan's electronic protected health information ("ePHI") as required by 45 C.F.R. § 164.308(a)(1)(ii)(A) and known as a Risk Analysis. The Risk Analysis shall incorporate all locations that maintain The Plan's PHI and must include an assessment of the risks to the security of ePHI in electronic equipment, data systems, and programs and applications controlled, administered, owned, or shared by The Plan, that create, receive, maintain, or transmit ePHI. Prior to conducting the Risk Analysis, The Plan shall develop a complete inventory of all of locations, electronic equipment, data systems, programs, applications, and other information technology assets that create, receive, maintain, or transmit ePHI, which will then be incorporated into their Risk Analysis.

2. Within sixty (60) days of the Effective Date, The Plan shall submit to HHS the scope and methodology by which they propose to conduct the Risk Analysis described in paragraph V.A.1. HHS shall notify The Plan whether the proposed scope and methodology is or is not consistent with 45 C.F.R. § 164.308(a)(1)(ii)(A).

3. The Plan shall provide the Risk Analysis, consistent with paragraph V.A.I., to HHS within sixty (60) days of HHS' approval of The Plan's methodology described in paragraph V.A.2 for HHS' review. HHS will inform The Plan's Contact in writing as to whether HHS approves of the Risk Analysis or, if necessary to ensure compliance with 45 C.F.R. § 164.308(a)(1)(ii)(A), requires revisions to the Risk Analysis. If HHS requires revisions to the Risk Analysis, HHS shall provide The Plan's

Contact with a detailed, written explanation of such required revisions and with comments and recommendations in order for The Plan to be able to prepare a revised Risk Analysis. Upon receiving notice of required revisions to the Risk Analysis from HHS and a description of any required changes to the Risk Analysis, The Plan shall have thirty (30) days in which to revise their Risk Analysis accordingly and submit the revised Risk Analysis to HHS for review and approval. This submission and review process shall continue until HHS approves the Risk Analysis.

B. Policies and Procedures

1. The Plan shall review and, to the extent necessary, revise its current Privacy, Security, and Breach Notification Rule Policies and Procedures ("Policies and Procedures") to comply with the Federal standards that govern the privacy and security of individually identifiable health information (45 C.F.R. Part 160 and Subparts A, C, D and E of Part 164, the "Privacy Rule", "Security Rule", and "Breach Notification Rule"). The Plan's policies and procedures shall include, but not be limited to, the minimum content set forth in Section V.D.

2. The Plan shall provide any revised Policies and Procedures, consistent with section V.B.1 above to HHS for review and approval within sixty (60) days of HHS' approval of the Risk Analysis as required by A.1. Upon receiving any recommended changes to the Policies and Procedures from HHS, The Plan shall have thirty (30) days to revise them accordingly and provide the revised Policies and Procedures to HHS for review and approval. This process shall continue until HHS approves such revised policies and procedures.

3. The Plan shall implement such policies and procedures within thirty (30) days of HHS' final approval.

C. Distribution of Policies and Procedures

1. The Plan shall distribute the Policies and Procedures identified in Section V.B. to all members of the workforce who have access to PHI within thirty (30) days of HHS' approval of such policies and to new members of the workforce within thirty (30) days of their beginning of service.

2. The Plan shall require, at the time of distribution of the Policies and Procedures, a signed written or electronic initial compliance certification from all members of the workforce stating that the workforce members have read, understand, and shall abide by such policies and procedures.

3. The Plan shall assess, update, and revise, as necessary, the Policies and Procedures at least annually (and more frequently if appropriate). The Plan shall provide such revised policies and procedures to HHS for review and approval. Upon receiving any recommended changes to the Policies and Procedures from HHS, The Plan shall have thirty days to revise such policies and procedures accordingly and provide the revised Policies and Procedures to HHS for review and approval. Within thirty days of the effective date of any approved substantive revisions, The Plan shall distribute the revised Policies and Procedures to all members of its workforce, and to new members as required by Section V.D.1, and shall require new compliance certifications.

4. The Plan shall not provide access to ePHI to any member of its workforce if that workforce member has not signed or provided the written or electronic certification required by paragraphs 2 and 3 of this Section.

D. Minimum Content of the Policies and Procedures

The Policies and Procedures shall include, but not limited to, measures to address the following Privacy, Security, and Breach Notification Rule provisions:

1. Documentation - 45 C.F.R. § 164.530(j), including a process to ensure proper documentation of:

    a. the policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of the Privacy and Breach Notification Rules;

    b. communication is required by the Privacy Rule to be in writing;

    c. an action, activity, or designation is required by the Privacy Rule to be documented;

    d. documentation sufficient to meet its burden of proof under § 164.414(b).

2. Risk Analysis - 45 C.F.R. § 164.308(a)(1)(ii)(A), including a process(es) to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by The Plan.

3. Information System Activity Review - 45 C.F.R. § 164.308(a)(1)(ii)(D), including a process(es) for the regular review of all records of information system activity, such as audit logs, access reports, and

security incident tracking reports, collected by The Plan and processes for evaluating when the collection of new or different record that need to be included in the review, including parameters for reviewing systems' activity, the frequency of reviews, and procedures for documenting and reporting results of such reviews.

4. Protection from Malicious Software- 45 C.F.R. § 164.308(a)(5)(ii)(B), including procedures for guarding against detecting, and reporting malicious software.

5. Access Control - 45 C.F.R. § 164.312(a)(1), including prov1s1ons to address access between systems, such as network or portal segmentation, provisions to limit access to ePHI to individuals and software programs granted access rights, and provisions to enforce password management requirements.

6. Contingency Plan - 45 CFR § 164.308(a)(7)(ii)(A)-(E), including a process(es) for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain ePHI. Process to include procedures to create and maintain exact copies of ePHI, procedures to restore any loss of data, procedures to enable continuation of critical business processes prior to the incident, periodic testing and revision of plans, and assess the relative criticality of specific applications and data in support of other contingency plan components.

7. Documentation - 45 C.F.R. § 164.316(b)(i), including a process to ensure proper documentation of

    a. The policies and procedures implemented to comply with the Security Rule in written form; and
    b. Actions, activities, or assessments that are required to be documented under the Security Rule

E. Reportable Events

During the Compliance Term, The Plan shall, upon receiving information that a workforce member may have failed to comply with its Privacy, Security or Breach Notification Rule Policies and Procedures, or that a business associate may have failed to comply with the provisions of the business associate agreement, as applicable, promptly investigate this matter. If The Plan determines, after review and investigation, that a member of its workforce, or a business associate that has agreed to comply with policies and procedures under Section V.C. has failed to comply with these policies and procedures, The Plan shall notify in writing HHS within thirty (30) days. Such violations

shall be known as Reportable Events. The report to HHS shall include the following information:

a. complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the policies and procedures implicated; and

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

F. Training

1. The Plan shall provide HHS with training materials addressing the requirements of the Privacy, Security, and Breach Notification Rules, intended to be used for all workforce members within sixty (60) days of the implementation of the Policies and Procedure required by Section V.B. above.

2. Upon receiving notice from HHS specifying any required changes, The Plan shall make the required changes and provide revised training materials to HHS within thirty (30) days.

3. Upon receiving approval from HHS, The Plan shall provide training using the approved training materials for all workforce members within sixty (60) days of HHS' approval and at least every twelve (12) months thereafter. The Plan shall also provide such training to each workforce member within thirty (30) days of the commencement of such workforce member's service.

4. Each workforce member shall certify, in writing or in electronic form, that she or he has received and understands the required training. The training certification shall specify the date on which training was received. All course materials shall be retained in compliance with Section VII below.

5. The Plan shall review the training annually, and, where appropriate, update the training to reflect changes in Federal law or HHS guidance, any issues discovered during internal or external audits or reviews, and any other relevant developments.

6. The Plan shall not provide access to ePHI to any workforce member if that workforce member has not signed or provided the written or

electronic certification required by paragraph V.F.4 within a reasonable period of time after completion of such training.

## VI. Implementation Report and Annual Reports

A. Implementation Report. Within sixty (60) days after the receipt of HHS' approval of the training materials required by Section V.F., The Plan 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 The Plan attesting that training materials have been developed, distributed and explained to all appropriate members of the workforce, and that The Plan has obtained all of the compliance certifications in accordance with paragraph V.F.4;

2. A copy of all training materials used for the training required by this CAP, a description of the training, including a summary of the topics covered, the length of the session(s) and a schedule of when the training session(s) were held;

3. An attestation signed by an owner or officer of The Plan attesting that all workforce members have completed the initial training required by this CAP and have executed the training certifications required by Section V.F.4;

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

5. An attestation signed by an owner or officer of The Plan 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." The Plan also shall submit to HHS Annual Reports with respect to the status of and findings regarding The Plan's compliance with this CAP for each of the three (3) year Reporting Periods. The Plan shall submit each Annual Report

to HHS no later than sixty (60) days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. A schedule, topic outline, and copies of the training materials for the training programs attended in accordance with this CAP during the Reporting Period that is the subject of the report;

2. An attestation signed by an owner or officer of The Plan attesting that The Plan is obtaining and maintaining written or electronic training certifications from all persons who are required to attend training pursuant to the requirements set forth in this CAP;

3. A summary of Reportable Events (defined in Section V.E) identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events;

4. An attestation signed by an owner or officer of The Plan 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

The Plan 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

The Plan is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions

The Plan 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. The requirement may be waived by OCR only.

B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty.

The parties agree that a breach of this CAP by The Plan constitutes a breach of the Agreement. Upon a determination by HHS that The Plan has breached

this CAP, HHS may notify The Plan of: (1) The Plan's breach; and (2) HHS' intent to impose a 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. The Plan's Response.

The Plan shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. The Plan 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 thirty (30) calendar day period, but that: (a) The Plan has begun to take action to cure the breach; (b) The Plan is pursuing such action with due diligence; and (c) The Plan has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP.

If at the conclusion of the thirty (30) calendar day period, The Plan fails to meet the requirements of Section VIII.C. of this CAP to HHS' satisfaction, HHS may proceed with the imposition of a CMP against The Plan 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 The Plan in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

**For Spencer Gifts LLC Flexible Benefits and Welfare Benefit Plans**

/s/ 05/07/2026

Kevin Mahoney
Senior Vice President
Spencer Gifts LLC

Date

**For United States Department of Health and Human Services**

/s/ 05/20/2026

Barbara Stampul
Regional Manager
Enforcement Division
Office for Civil Rights

Date