CYBERSECURITY ADDENDUM

This Cybersecurity Addendum ("**CSA**") is between Conagra Brands, Inc. and its affiliates (Collectively, "**Conagra**") and the service provider accepting these terms and conditions ("**Service Provider**") (collectively, the "**Parties**"). Where the Parties are subject to an existing written agreement (the "**Agreement**"), this CSA is intended to supplement such existing Agreement, and is hereby incorporated by reference into the Agreement.

WHEREAS, the Parties written Agreement may permit Service Provider, its employees, and/or agents to access or manage Conagra's information assets in order to provide the services set forth in the Agreement ("**Services**"); and

WHEREAS, this CSA sets forth specific controls that must be implemented by Service Provider when accessing or managing Conagra's information assets for the purpose of protecting such assets against cybersecurity threats, including without limitation, access by unauthorized Persons, loss or non-availability, manipulation of falsification, or other malicious or unintended outcomes; and

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which the Parties acknowledge, the Parties agree as follows:

1. **Definitions**. The following capitalized terms as used herein shall be defined as follows:

   (a) "**Affiliate**" means any Person that controls, is controlled by or is under common control with another Person. For purposes of the defined term Affiliate, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

   (b) "**Authorized User**" means any employee, contractor, agent or other Person that participates in the business operations of Service Provider and is authorized to access and use any Information Systems and data of Service Provider or Conagra in the performance of the Services.

   (c) "**Cybersecurity Event**" means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information, including without limitation Nonpublic Information, stored on such Information System.

   (d) "**Information System**" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

   (e) "**Multi-factor Authentication**" means authentication through verification of at least two of the following types of authentication factors:

      (1) knowledge factors, such as a password;
      (2) possession factors, such as a token or text message on a mobile phone; or
      (3) inherence factors, such as a biometric characteristic.

   (f) "**Nonpublic Information**" shall mean Conagra electronic information provided to or accessed by Service Provider that is not Publicly Available Information including, as applicable:

      (1) information of a confidential and proprietary nature, including, without limitation, financial information; products; techniques; processes; formulae; product specifications; know-how; recipes; inventions; patent applications; designs; drawings; samples; marketing and manufacturing plans, pricing, analyses, strategies, and forecasts; concepts; ideas; names, addresses or other supplier, customer or employee information; analyses,

reports, summaries, diagrams, descriptions, memoranda, any information related to dispute resolution between the Parties; and other materials derived, summarized, or extracted from any of the foregoing; or

(2) any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

a. social security number;
b. drivers' license number or non-driver identification card number;
c. account number, credit or debit card number;
d. any security code, access code or password that would permit access to an individual's financial account; or
e. biometric records;

(3) any information or data, except age or gender, in any form or medium created by or derived from an individual and that relates to:

a. the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family;
b. the provision of health care to any individual; or
c. payment for the provision of health care to any individual.

(g) "**Penetration Testing**" means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Service Provider's Information Systems.

(h) "**Person**" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(i) "**Publicly Available Information**" means information which is or becomes publicly available through no breach of this CSA or the Agreement by Service Provider.

(j) "**Risk Assessment**" means the risk assessment(s) that Service Provider is required to conduct under Section 7.

(k) "**Risk-based Authentication**" means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(l) "**Security Audits**" means the Conagra audit of Service Provider's relevant operations, facilities, and Information Systems, as described in Section 19 of this CSA, for the purpose of confirming that Service Provider has complied with the requirements of this CSA

(m) "**Third Party Service Provider(s)**" means a Person that:
(1) is not an Affiliate of the Service Provider;
(2) provides services to the Service Provider; and
(3) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to Service Provider.

2. **Cybersecurity Program**.

(a) Service Provider shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of Service Provider's Information Systems and any Non-public Information contained therein.

(b) The cybersecurity program shall be based on Service Provider's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on Service Provider's Information Systems;
(2) use defensive infrastructure and the implementation of policies and procedures to protect Service Provider's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
(3) detect Cybersecurity Events;
(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;
(5) recover from Cybersecurity Events and restore normal operations and services; and
(6) fulfill applicable regulatory reporting obligations.

(c) All documentation and information relevant to Service Provider's cybersecurity program shall be made available to Conagra upon request.

3. **Cyber Security Policy**. Service Provider shall implement and maintain a written policy or policies setting forth Service Provider's procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The policy(s) shall be based on the Service Provider's Risk Assessment(s) and address the following areas to the extent applicable to Service Provider's operations:

(a) information security;
(b) data governance and classification;
(c) asset inventory and device management;
(d) access controls and identity management;
(e) business continuity and disaster recovery planning and resources;
(f) systems operations and availability concerns;
(g) systems and network security;
(h) systems and network monitoring;
(i) systems and application development and quality assurance;
(j) physical security and environmental controls;
(k) customer data privacy;
(l) Third Party Service Provider management;
(m) Risk Assessment; and
(n) incident response.

4. **Penetration Testing and Vulnerability Assessments**. The cybersecurity program for Service Provider shall include monitoring and testing, developed in accordance with Service Provider's Risk Assessment, designed to assess the effectiveness of Service Provider's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Service Provider shall conduct:

(a) annual Penetration Testing of its Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in its Information Systems based on the Risk Assessment.

Service Provider shall (i) log vulnerability scan reports; (ii) conduct periodic reviews of vulnerability scan reports over time; (iii) use patch management and software update tools for the Service Provider Information Systems; (iv) prioritize and remediate vulnerabilities by risk; and (v) use compensating controls if no patch or remediation is immediately available.

5. **Audit Trail**. Service Provider shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

   (a) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of Service Provider; and

   (b) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of Service Provider.

   Service Provider shall maintain records required by subsection (a) for not fewer than five (5) years and shall maintain records required by subsection (b) for not fewer than three (3) years.

6. **Access Privileges and Account Management**.

   (a) As part of its cybersecurity program, Service Provider shall limit user access privileges to Information Systems that provide access to Nonpublic Information to only those users with a need to access such Information Systems for the purpose of providing the Services, or internal business purposes related thereto, and shall periodically review such access privileges. Service Provider will promptly terminate its personnel's access within twenty-four (24) hours to such data when access is no longer required to provide the Services under the Agreement.

   (b) Service Provider will use reasonable measures to manage the creation, use, and deletion of all account credentials used to access Information Systems, including by implementing: (i) a segregated account with unique credentials for each user; (ii) strict management of administrative accounts; (iii) password best practices, including the use of strong passwords and secure password storage; and (iv) periodic audits of accounts and credentials.

7. **Risk Assessment**.

   (a) Service Provider shall conduct a periodic Risk Assessment of its Information Systems sufficient to inform the design of its cybersecurity program. Such risk assessment shall be updated as reasonably necessary to address changes to Service Provider's Information Systems, the Nonpublic Information contained therein, or its business operations. Service Provider's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of its business operations related to cybersecurity, the Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

   (b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

      (1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing Service Provider;
      (2) criteria for the assessment of the confidentiality, integrity, security and availability of Service Provider's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and
      (3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

(c) At a minimum, the Risk Assessment shall include site audits of the Information System and information security controls for all facilities used in complying with its obligations under this CSA, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices. Upon Conagra's written request, Service Provider shall make available to Conagra for review all of the following, as applicable: Service Provider's latest Payment Card Industry (PCI) Compliance Report, Statement on Standards for Attestation Engagements (SSAE) No. 18 audit reports for Reporting on Controls at a Service Organization, Service Organization Controls (SOC) Type 1, 2, or 3 audit reports, and any reports relating to its ISO/IEC 27001 certification. Conagra shall treat such audit reports as Service Provider's confidential information under this CSA. Service Provider will promptly address any exceptions noted on the SOC reports, or other audit reports, with the development and implementation of a corrective action plan by Service Provider's management.

8. **Cybersecurity Personnel and Intelligence**. Service Provider shall:

(a) utilize qualified cybersecurity personnel of Service Provider, an Affiliate or a Third Party Service Provider sufficient to manage its cybersecurity risks and to perform or oversee the performance of the cybersecurity functions specified in this CSA;

(b) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(c) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

9. **Third Party Service Provider Policies and Procedures**.

(a) Service Provider shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall address to the extent applicable:

(1) the identification and Risk Assessment of Third Party Service Providers;
(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for Service Provider to do business with the Third Party Service Provider;
(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and
(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers, including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider’s policies and procedures for access controls, including its use of Multi-factor Authentication as required herein, to limit access to relevant Information Systems and Nonpublic Information;
(2) the Third Party Service Provider’s policies and procedures for use of encryption as required by this CSA to protect Nonpublic Information in transit and at rest;
(3) notice to be provided to the Service Provider in the event of a Cybersecurity Event directly impacting Service Provider’s Information Systems or the Nonpublic Information being held by the Third Party Service Provider; and
(4) representations and warranties substantially similar to the representations and warranties presented in Section 16 of this CSA addressing the Third Party Service Provider’s cybersecurity policies and procedures that relate to the security of its Information Systems and Nonpublic Information.

10. **Multi-factor Authentication**.

    (a) Based on its Risk Assessment, Service Provider shall use effective controls, which may include Multi-factor Authentication or Risk-based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

    (b) Multi-factor Authentication shall be utilized for any individual accessing Service Provider's internal networks from an external network, unless Service Provider has assessed and approved in writing the use of reasonably equivalent or more secure access controls.

11. **Limitations on Data Retention**. As part of its cybersecurity program, Service Provider shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

12. **Data Loss Prevention**. Service Provider will use reasonable data loss prevention measures to identify, monitor, and protect Non-public Information in use, in transit, and at rest. Such data loss prevention processes and tools will include: (i) automated tools to identify attempts of data exfiltration; (ii) the prohibition of, or secure and managed use of, portable devices; and (iii) use of certificate-based security.

13. **Monitoring and Training**. As part of its cybersecurity program, Service Provider shall:

    (a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

    (b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by Service Provider in its Risk Assessment.

14. **Encryption and Pseudonymization**.

    (a) As part of its cybersecurity program, based on its risk assessment, Service Provider shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by Service Provider both in transit over external networks and at rest.

    (b) Service Provider will, where possible and consistent with the services provided under the Agreement, use industry standard and appropriate pseudonymization techniques to protect Non-public Information.

15. **Incident Response Plan**.

    (a) As part of its cybersecurity program, Service Provider shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of its Information Systems or the continuing functionality of any aspect of its business or operations.

    (b) Such incident response plan shall address the following areas:

        (1) the internal processes for responding to a Cybersecurity Event;
        (2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;
(4) external and internal communications and information sharing;
(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

16. **Security Standards Representations and Warranties**.

(a) Service Provider represents and warrants that it has implemented administrative, physical, and technical safeguards to protect Non-public Information from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices (including/specifically the International Organization for Standardization's standards: ISO/IEC 27001 – Information Security Management Systems – Requirements and ISO/IEC 27002 – Code of Practice for International Security Management, the Control Objectives for Information and related Technology (COBIT) standards, or the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and shall ensure that all such safeguards, including the manner in which Non-public Information is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this CSA.

(b) If, in the course of its engagement by Conagra, Service Provider has access to or will collect, access, use, store, process, dispose of, or disclose credit, debit, or other payment cardholder information, Service Provider represents and warrants that it shall remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Service Provider's sole cost and expense.

(c) Service Provider represents and warrants that its safeguards for the protection of Non-public Information include: (i) limiting access of Non-public Information to Authorized Users; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment; (vi) encrypting Non-Public Information stored on any mobile media; (vii) encrypting Non-public Information when transmitted over public or wireless networks; (viii) strictly segregating Non-public Information from information of Service Provider or its other customers so that Non-public Information is not commingled with any other types of information; (ix) conducting Risk Assessments, Penetration Testing, and vulnerability scans and promptly implementing, at Service Provider's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xi) providing appropriate privacy and information security training to Service Provider's employees; (xii) monitoring, detecting, and restricting the flow of Non-public Information on a multilayered basis within the Information Systems using tools such as firewalls, proxies, and network-based intrusion detection systems.

(d) Service Provider represents and warrants that it shall at all times cause such Authorized Users to abide strictly by Service Provider's obligations under this CSA. Service Provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use, or disclosure of Non-public Information by any of Service Provider's officers, partners, principals, employees, agents, or contractors.

(e) Service Provider represents and warrants that any software used in connection with the processing of Non-public Information is or has been developed using secure software development practices, including by: (i) segregating development and production environments; (ii) filtering out potentially malicious character sequences in user inputs; (iii) using secure communication techniques, including encryption; (iv) using sound memory management practices; (v) using web application firewalls to address common web application attacks such as cross-site scripting, SQL injection and command injection; (vi) implementing the OWASP Top Ten recommendations, as applicable; (vii) patching of software; (viii) testing object code and source code for common coding errors and vulnerabilities using code analysis tools; (ix) testing of web applications for vulnerabilities using web application scanners; and (x) testing software for performance under denial of service and other resource exhaustion attacks.

17. **Cybersecurity Event Procedures**.

(a) Service Provider shall:

(1) provide Conagra with the name and contact information for one or more employees/security operations or other service desk of Service Provider which shall serve as Conagra's primary security contact and shall be available to assist Conagra twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Cybersecurity Event;
(2) notify Conagra of a Cybersecurity Event as soon as practicable, but no later than twenty-four (24) hours after Service Provider becomes aware of it; and
(3) notify Conagra of any Cybersecurity Event by emailing Conagra at Cybersecurity@conagra.com and Privacy@Conagra.com, with a copy by email to Service Provider's primary business contact within Conagra.

(b) Immediately following Service Provider's notification to Conagra of a Cybersecurity Event, the parties shall coordinate with each other to investigate the Cybersecurity Event. Service Provider agrees to fully cooperate with Conagra in Conagra's handling of the matter, including, without limitation: (i) assisting with any investigation, including the completion of a breach notification questionnaire as requested by Conagra; (ii) providing Conagra with physical access to the facilities and operations affected; (iii) facilitating interviews with Service Provider's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Conagra.

(c) As soon as reasonably practical following Service Provider's request, Service Provider shall provide Conagra with a network diagram that outlines Service Provider's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under this CSA and the Agreement, including, without limitation: (i) connectivity to Conagra and all third parties who may access Service Provider's network to the extent the network contains Non-public Information; (ii) all network connections, including remote access services and wireless connectivity; (iii) all access control measures (for example, firewalls, packet filters, intrusion detection and prevention services, and access-list-controlled routers); (iv) all backup or redundant servers; and (v) permitted access through each network connection. In lieu of providing Conagra with the network diagram as described above, Service Provider may opt to have a reputable third-party digital forensics firm perform a breach investigation. Such breach investigation shall be performed at Service Provider's sole cost and expense and Service Provider shall provide a copy of the results of the breach investigation to Conagra promptly upon completion.

18. **Business Continuity and Disaster Recovery**. Service Provider will provide appropriate continuity and recovery plans to ensure (i) Service Provider can restore availability and access to Non-public Information as soon as possible in the event of an incident, including without limitation a Cybersecurity Event; and (ii) continued service in an event that impacts Service Provider's data centers or offices providing the contracted services, and to the extent applicable, in accordance with any service level agreements. Such plans must be tested at least annually.

19. **Audit Rights**. During the term of the Agreement, and thereafter for as long as Service Provider retains Non-Public Information, Conagra will be entitled to conduct audits of Service Provider's relevant operations, facilities, and

Information Systems for the purpose of confirming that Service Provider has complied with the requirements of this CSA. Any Security Audit shall be scheduled and conducted during normal business hours and shall not unreasonably interfere with Service Provider's business activities. In the event that any Security Audit results in the discovery of material security risks to Non-public Information, or violations of applicable federal or state laws, rules, and regulations, Service Provider shall (i) respond to Conagra in writing with Service Provider's plan to promptly take reasonable measures and corrective actions necessary to effectively eliminate the risk or cure the violation at no cost to Conagra; and (ii) allow Conagra to review any Information System related thereto which contains or interacts in any way with Non-public Information. Unless the parties mutually agree in writing to a longer period of time, Service Provider shall have five (5) business days to cure such security risk or violation. Conagra's right to conduct a Security Audit, and any exercise of such right, shall not in any way diminish or affect Service Provider's duties and liabilities under this Agreement.

20. **Return or Destruction of Information**. At any time during the term of the Agreement, at Conagra's written request or upon the termination or expiration of this Agreement, Service Provider shall, and shall instruct all Authorized Users and Third Party Service Providers to, promptly return to Conagra all copies, whether in written, electronic, or other form or media, of Non-public Information in its possession or the possession of such Authorized Users or Third Party Service Providers, or securely dispose of all such copies, and certify in writing to Conagra that such Non-public Information has been returned to Conagra or disposed of securely. Service Provider shall comply with all reasonable directions provided by Conagra with respect to the return or disposal of Non-public Information.

21. **Equitable Relief**. Service Provider acknowledges that any breach of its covenants or obligations set forth in this CSA may cause Conagra irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Conagra is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which Conagra may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Agreement to the contrary.

22. **Material Breach**. Service Provider's failure to comply with any of the provisions of this CSA is a material breach of the Agreement. In such event, Conagra may terminate the Agreement effective immediately upon written notice to the Service Provider without further liability or obligation to Conagra.

23. **Indemnification**. Service Provider shall defend, indemnify, and hold harmless Conagra and Conagra's parent company and their subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors, and permitted assigns (each, a "Conagra Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Conagra Indemnitee arising out of or resulting from Service Provider's failure to comply with any of its obligations under this CSA.