proofpoint.

Business Associate Agreement Addendum

This Business Associate Agreement Addendum ("***Addendum***") is entered into by and between the party identified below ("***Customer***") and Proofpoint, Inc., with an address at 925 W. Maude Avenue, Sunnyvale, California 94085 ("***Proofpoint***") (each, individually, a "***Party***" and both, collectively, the "***Parties***"). This Addendum is made a part of, and incorporated into, either: (1) the Proofpoint General Terms and Conditions and applicable Product Exhibit(s), (2) the end user license agreement (a EULA, clickwrap, or clickthrough agreement) accepted by Customer on customer's initial registration and access of the Proofpoint product or service, (3) any other written applicable agreement mutually agreed as between the Parties, or (4) the Proofpoint Evaluation Terms and Conditions by and between the Parties (the "***Proofpoint Agreement***"). The Effective Date of this Addendum is the date the last party executes the Addendum.

Accepted and agreed by Customer:		Accepted and agreed by **Proofpoint, Inc.**	
Signature:	_____	Signature:	DocuSigned by: Paul Auvil 2955B8CEBD2B45C...
Name:	_____	Name:	Paul Auvil, CFO
Date:	_____		
Company:	_____		
Address:	_____		
	_____		

WHEREAS, Customer has access to certain Proofpoint's products and services deployed via the Proofpoint Cloud known as Email Archiving (where the Email Appliances reside at Customer premises), Continuity, Email Protection, Targeted Attack Protection, Encryption, Email Data Loss Prevention, Cloud App Security Broker, Cloud App Defense, Email Fraud Defense, and Insider Threat Management (collectively, the "Services") pursuant to the Proofpoint Agreement; and

WHEREAS, during the Term, Customer's use of the Services may result in ePHI (as later defined) passing through the Services. As a result Proofpoint may have access to Protected Health Information (as defined in 45 CFR Section 160.103) which may be subject to the administrative simplification section of the Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191 (Aug. 21, 1996), and its implementing regulations, and the Health Information Technology for Economic and Clinical Health Act ("***HITECH***") (collectively, "***HIPAA***"); and

WHEREAS, the Parties desire to supplement and/or amend the Proofpoint Agreement only with respect to Proofpoint's receipt, use, disclosure, maintenance, and transmission of such Protected Health Information under the Proofpoint Agreement to allow Customer to comply with HIPAA.

NOW, THEREFORE, in consideration of the mutual covenants, provisions and agreements set forth below, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto agree as follows:

1. INTEGRATION, DEFINITIONS. This Addendum is made an integral part of, and is incorporated by reference into, the Proofpoint Agreement. To the extent of any conflict or inconsistency between a provision of the Proofpoint Agreement and this Addendum, this Addendum shall control. Certain data elements used to provide the Services may contain Personal Data that could be classified as PHI. Threats mimicking PHI do not equate to PHI, and notwithstanding anything to the contrary, to the extent of any conflict or inconsistency between a provision of this Addendum and the applicable Product Exhibit, the Product Exhibit shall control. Capitalized terms used in this Business Associate Addendum without separate definition shall have the meaning specified in the Proofpoint Agreement. Unless otherwise defined in this Addendum or the Proofpoint Agreement, all capitalized terms used in this Addendum have the respective meanings ascribed in the HIPAA regulations. "**ePHI**" shall mean Electronic Protected Health Information as defined in 45 CFR Section 160.103 and shall be limited to the ePHI Customer transmits in connection with the Services (hereinafter, "**PHI**"). "**Security Rule**" shall mean the Security Standards

for the Protection of Electronic Protected Health Information at 45 CFR Part 164 subpart C. **"Privacy Rule"** means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR 164 subpart E.

2. BACKGROUND, PURPOSE AND SCOPE.

This Addendum is made pursuant to, and shall hereby supplement and/or amend, the Proofpoint Agreement only with respect to Proofpoint's receipt, access, use, disclosure, maintenance or transmission of PHI under the Proofpoint Agreement. Except as so supplemented and/or amended by this Addendum, the terms of the Proofpoint Agreement shall continue unchanged and shall apply with full force and effect to govern the matters addressed in this Addendum and in the Proofpoint Agreement.

3. OBLIGATIONS OF THE PARTIES WITH RESPECT TO PHI.

3.1. Obligations of Proofpoint. Proofpoint shall:

a. not use or disclose PHI other than as permitted or required by the Proofpoint Agreement or this Addendum or as required by law;

b. implement appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of the PHI that Proofpoint creates, receives, maintains, or transmits on behalf of the Customer in accordance with the Security Rule and the Privacy Rule;

c. to the extent Proofpoint carries out Customer's obligations under HIPAA, comply with the requirements of HIPAA that apply to the Customer in the performance of such obligations, if any;

d. within a reasonable period of time report to Customer any: (i) access, acquisition, use or disclosure of PHI that is not provided for by the Proofpoint Agreement, this Addendum, or written approval of Customer, (ii) Security Incident, or (iii) Breach (as defined in 45 CFR Section 164.402) of unsecured PHI, following its discovery (as defined under 45 CFR Section 164.410(a)(2)) by Proofpoint, which report shall include, to the extent reasonably possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by Proofpoint to have been, accessed, acquired, used, or disclosed during the breach, provided that notice is hereby deemed given for Unsuccessful Security Incidents and no further notice of such Unsuccessful Security Incidents shall be given. For purposes of this Addendum, "Unsuccessful Security Incidents" mean, without limitation, pings and other broadcast attacks on Proofpoint's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, use, or disclosure of Protected Health Information. In the event of a Breach, Proofpoint shall cooperate with Customer in Customer's efforts to carry out Customer's notification and mitigation obligations under HIPAA, including providing Customer with information reasonably available for inclusion in notification to the individual under 45 CFR Section 164.404(c) at the time of the notification or promptly thereafter as information becomes available;

e. in performing its obligations in connection with the Proofpoint Agreement, access, use, disclose and/or request only the minimum PHI necessary to accomplish the intended purpose of the access, use, disclosure or request;

f. in accordance with 45 CFR Sections 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any agents and subcontractors to which PHI is disclosed, agree to the same restrictions, conditions, and requirements that apply to Proofpoint with respect to such information, including compliance with the Security Rule and Privacy Rule;

g. within ten (10) days of receiving a written request from Customer, make available to Customer PHI, if any, necessary for the Customer to respond to Individuals' requests for access to PHI about them (pursuant to 45 CFR Section 164.524) in the event that the PHI in Proofpoint's possession constitutes a

Designated Record Set, and within ten (10) days of receipt of a request for access directly from an Individual, forward the request to Customer;

h. within ten (10) days of receiving a written request from Customer, make available to Customer PHI for amendment, if any, pursuant to 45 CFR Section 164.526 and incorporate any amendments to the PHI in the event that the PHI in Proofpoint's possession constitutes a Designated Record Set and within ten (10) days of receipt of a request for amendment directly from an Individual, forward the request to Customer;

i. within ten (10) days of receiving a written request from Customer, make available to Customer the information required for Customer to provide an accounting of disclosures pursuant to 45 CFR Section 164.528, and within ten (10) days of receipt of a request for an accounting directly from an Individual, forward the request to Customer;

j. mitigate to the extent practical any known harmful effects caused by use or disclosure of PHI by Proofpoint and/or its agents and subcontractors in violation of the requirements of this Addendum;

k. as soon as reasonably practicable, but no later than thirty (30) days of receiving a written notice from Customer, return to Customer or destroy all PHI, and retain no copies, if it is feasible to do so; provided, however, in the event that Proofpoint determines that returning or destroying PHI is not feasible, Proofpoint shall provide to the Customer notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Proofpoint shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Proofpoint maintains such PHI;

l. upon Customer's request, provide Customer with access to and copies of any records, books, policies and procedures developed or utilized by Proofpoint regarding the protection of PHI, subject to applicable legal privileges, at Customer's sole cost and expense, during Proofpoint's regular business hours at a time mutually agreed to by the parties, and no more than once per calendar year, for the purposes of determining Proofpoint's compliance with this Addendum;

m. make its internal practices, books, and records available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with HIPAA, subject to attorney-client and other applicable legal privileges;

n. have its employees take security awareness training upon hire and thereafter at least on an annual basis; and

o. provide role-based access to its employees for the systems used to provide the Services.

3.2. Permitted Uses and Disclosures of PHI by Proofpoint. Except as otherwise specified in this Addendum, Proofpoint shall access, acquire, use, and/or disclose PHI only as be reasonably necessary to perform its obligations under the Proofpoint Agreement. ALL OTHER ACCESS, ACQUISITION, USES AND/OR DISCLOSURES OF PHI, INCLUDING, BUT NOT LIMITED TO DE-IDENTIFICATION OF PHI, ARE PROHIBITED UNLESS EXPRESSLY PERMITTED IN WRITING BY CUSTOMER. Nothing in this Addendum shall be construed to prohibit Proofpoint's disclosure to Customer of PHI obtained from Customer or created or obtained on behalf of Customer, or disclose the PHI in its possession as required by law; provided, (a) Proofpoint obtains reasonable assurances in writing from the third party to whom the PHI is disclosed that (i) the PHI will be held confidentially in the manner specified by HIPAA and used or further disclosed only as required by law and (ii) the third party will notify Proofpoint of any instances of which it is aware in which the confidentially of unsecured PHI has been breached and (b) to the extent permitted by law, Proofpoint provides prior notice of the proposed disclosure to Customer and an opportunity for Customer to object to the disclosure.

3.3. Obligations of Customer. Except in sole connection with the Services, Customer shall not provide or send PHI in any form to Proofpoint. Proofpoint does not act as, or have the obligations of, a Business Associate with respect to Protected Health Information that Customer transmits to Proofpoint outside of the Services. Customer shall use commercially reasonable efforts: (a) to notify Proofpoint of any limitations(s) in Customer's notice of privacy practices under 45 CFR Section 164.520 to the extent that such limitations may affect Proofpoint's permitted or required uses and disclosures of the PHI; (b) to notify Proofpoint of any changes in, or revocation of, permission by an Individual to use or disclose PHI to the extent that such event may affect Proofpoint's permitted or required uses and disclosures; (c) to obtain from Individuals any required consent or authorization necessary for Proofpoint and Customer to fulfill their respective obligations under HIPAA and this Addendum; and (d) to not request Proofpoint to use or disclose PHI in any manner that would not be permissible under HIPAA if done by the Customer, except as set forth in Section 3.2 above.

3.4. Effect of Changes to HIPAA. To the extent that any relevant provision of HIPAA is amended in a manner that changes the obligations of the Parties that are embodied in the terms of this Addendum, the Parties shall negotiate in good faith appropriate amendment(s) to this Addendum to give effect to such revised obligations.

4. TERM AND TERMINATION.

4.1. Term. The term of this Addendum shall be effective as of the Effective Date and shall terminate when all of the PHI provided by the Customer to Proofpoint, or created or received by Proofpoint on behalf of the Customer, is destroyed or returned to the Customer, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with this Addendum.

4.2. Termination for Cause. Upon the Customer's knowledge of a material breach of this Addendum by Proofpoint, the Customer shall provide an opportunity for Proofpoint to cure the breach or end the violation. The Customer may terminate this Addendum and the Proofpoint Agreement if the Proofpoint does not cure the breach or end the violation within the time specified by the Customer, or immediately terminate this Addendum if cure or end of the violation is not possible.

4.3. Effect of Termination. Except as provided in this Section 4.3, upon termination of this Addendum or the Proofpoint Agreement, for any reason, the terms of 3.1(k) shall apply.

5. MISCELLANEOUS.

5.1. Interpretation. The terms of this Addendum shall prevail in the case of any conflict with the terms of the Proofpoint Agreement. Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits Customer to comply with applicable laws protecting the privacy, security and confidentiality of the PHI.

5.2. Survival. Notwithstanding any other provision of this Addendum to the contrary, the obligations of Proofpoint under this Addendum, including but not limited to Articles 1, 2, 3, and 5 and Section 4.3 shall survive termination of this Addendum and continue indefinitely solely with respect to PHI Proofpoint retains in accordance with this Addendum.

5.3. Regulatory references. Subject to Section 3.4, a reference in this Addendum to HIPAA or a section in HIPAA means that section as in effect as of the Effective Date.

5.4. No Third Party Beneficiaries. Nothing in this Addendum shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.