FEDERAL END USER LICENSE TERMS

These Federal End User License Terms shall apply to the use of Proofpoint Products by Customer pursuant to a subscription license. These End User License Terms are made expressly a part of the prime procurement contract with the Customer.

1. Definitions. The following terms apply to each Public Sector Customer ("Customer") license of Proofpoint Products from the Public Sector Reseller or Distributor ("Contractor") under the applicable government prime contract:

"Customer" means only the Ordering Activity under GSA Schedule contracts identified in the Purchase Order, Statement of Work, or similar document which has purchased the Proofpoint Product subscription license for its internal purposes and does not include any other agency or governmental subdivision unless expressly stated in this Agreement or the Proofpoint quote accompanying the purchase order.

"Documentation" means the technical description of the Proofpoint Product(s) contained in the then-current Product Terms.

"'**Government**' means when this designation appears in a Proofpoint Product SKU, the Proofpoint Product (or Product bundle) includes one or more Proofpoint Products that are delivered inside the Federal Risk and Authorization Management Program [FedRAMP]. Refer to the FedRAMP Marketplace https://marketplace.fedramp.gov/products for those specific Proofpoint Products delivered inside FedRAMP."

"Proofpoint Products" means the appliance, service or software listed in the Contractor's Schedule Price List by and licensed by Customer from Proofpoint, Inc. ("Proofpoint") pursuant to a Customer Purchase Order ("Order").

"**Product Terms**" means the descriptions of Proofpoint Products and related terms that are incorporated here in full as Exhibit 3.

"**Service**" means any Proofpoint Product licensed on a hosted basis as software-as-a-service.

"**Software**" means any Proofpoint binary software programs licensed by Proofpoint to Customer, together with all the Software Updates.

"User" means Customer's employees, agents, contractors, consultants or other individuals who are licensed to use the Proofpoint Product, and each User must be assigned a separate account on Customer's email server for sending or receiving messages or data within Customer's email system or network, or if applicable, login credentials for Customer's social media accounts.

2. License. Customer is granted a limited term, non-sublicensable, non-transferable, and non- exclusive license to access or use the Proofpoint Products licensed by Customer from Contractor during the applicable subscription term, for its intended purposes, solely for Customer's internal business purposes and not for further use by or disclosure to third parties and in accordance with the Proofpoint Products Documentation and any applicable federal laws or regulations. Customer's right to access or use Proofpoint Products is limited to those parameters set forth in the applicable Order provided to Proofpoint including, but not limited to the maximum number of Users ("Licensed User Count") (and storage if applicable) for each module and the type of deployment (i.e., SaaS or appliance). These EULA terms are made expressly a part of the prime contract with the Customer.

U.S. Government Users. Product and SaaS includes "Commercial Computer Software" and "Commercial Computer Software Documentation." In accordance with Section 12.212 of the Federal Acquisition Regulations (FAR) and Sections 227.7202-1 through 227.7202-4 of the Defense FAR Supplement (DFARS), any use, duplication, modification, distribution, disclosure and all other license rights of Product or SaaS by the U.S. Government or any of its agencies shall be governed by and subject to all of the terms, conditions, restrictions, and limitations of the Proofpoint license agreement. Use of Product or SaaS constitutes agreement by the U.S. Government that Product or SaaS includes "commercial computer software" and "commercial computer software documentation" per the FAR/DFAR; and renders the Proofpoint license agreement enforceable. If for any reason Product or SaaS is not considered 'commercial' per the FAR; or, the Proofpoint license agreement otherwise is deemed not to apply, the Product or SaaS will be deemed to be provided with "Restricted Rights" as defined in

FAR 52.227-14(a) and FAR 52.227-14(g)(4) (Alt III), or DFARS 252.227-7014(a)(15) and DFARS 252.227-7014(b)(3), as applicable. For U.S. Government Users, the Government shall have the right to use, duplicate or disclose Technical Data which is accessed, developed, or delivered under the contract, for the acquiring agency's internal purposes only, per FAR 12.211 Technical data. For contracts governed by the DFARS, the Government shall have the license rights for Technical Data as provided under DFAR 252.227-7015 (b)(Technical Data–Commercial Items).

3. License Restrictions.

Customer will not and will not allow any third party to:

a) copy, modify, or create derivative works of the Proofpoint Products or Proofpoint Products Documentation;

b) reverse engineer, decompile, translate, disassemble, or discover the source code of all or any portion of the Proofpoint Products except and only to the extent permitted by applicable federal law notwithstanding this limitation, provided however, that in any case, Customer shall notify Proofpoint in writing prior to any such action and give Proofpoint reasonable time to adequately understand and meet the requested need without such action being taken by Customer;

c) remove, alter, cover or obscure any notice or mark that appears on the Proofpoint Products or on any copies or media;

d) sublicense, distribute, disclose, rent, lease or transfer to any third party any Proofpoint Products;

e) export any Proofpoint Products in violation of U.S. laws and regulations;

f) attempt to gain unauthorized access to, or disrupt the integrity or performance of, a Proofpoint Product or the data contained therein;

g) access a Proofpoint Product for the purpose of building a competitive product or service or copying its features or user interface;

h) use a Proofpoint Product, or permit it to be used, for purposes of: (a) product evaluation, benchmarking or other comparative analysis intended for publication outside the Customer's organization without Proofpoint's prior written consent; (b) infringement or misappropriation of the intellectual property rights of any third party or any rights of publicity (e.g. a person's image, identity, and likeness) or privacy; (c) violation of any federal law, statute, ordinance, or regulation (including, but not limited to, the laws and regulations governing export/import control, unfair competition, anti- discrimination, and/or false advertising); (d) propagation of any virus, worms, Trojan horses, or other programming routine intended to damage any system or data; and/or (e) filing copyright or patent applications that include the Proofpoint Product and/or Documentation or any portion thereof; or

i) upload or download, post, publish, retrieve, transmit, or otherwise reproduce, distribute or provide access to information, software or other material which: (i) is confidential or is protected by copyright or other intellectual property rights, without prior authorization from the rights holder(s); (ii) is defamatory, obscene, contains child pornography or hate literature; or (iii) constitutes invasion of privacy, appropriation of personality (e.g. image, identity, likeness), or unauthorized linking or framing.

Proofpoint Products are for use with normal business messaging traffic only, and Customer shall not use the Proofpoint Products for the machine generated message delivery of bulk, unsolicited emails or in any other manner not prescribed by the applicable Proofpoint Products Documentation. Proofpoint shall have the right to monitor and reset harmful outbound email configuration settings impacting the Proofpoint platform.

4. Customer Responsibilities. Customer is responsible for (i) all activities conducted under its user logins; (ii) obtaining and maintaining any Customer equipment and any ancillary services needed to connect to, access or otherwise use the Proofpoint Products and ensuring that the Customer equipment and any ancillary services are (a) compatible with the Proofpoint Products and (b) comply with all configuration requirements set forth in the applicable Proofpoint Product Documentation; and (iii) complying with all federal laws, rules and regulations regarding the management and administration of its electronic messaging system, including but not limited to, obtaining any required consents and/or acknowledgements from its employees, agents, consultants and/or independent contractors (collectively referred to as "personnel," hereinafter) and service providers (if applicable) in managing its electronic messaging system and/or social media systems (as applicable). Customer shall be solely responsible for any damage or loss to a third party resulting from the Customer's data, or where Customer's use of the Proofpoint Products is in violation of federal law, or of this Agreement, or infringe the intellectual property rights of, or has otherwise harmed, such third party.

Customer shall (i) take all necessary measures to ensure that its users use Proofpoint Products in accordance with the terms and conditions of this Agreement; and (ii) in the case of any purchase of Proofpoint Secure Share, users of the Proofpoint Product will need to register to use the Secure Share. For the purposes of Proofpoint's compliance with its obligations under this Agreement, Customer consents to and authorizes Proofpoint (and its authorized subcontractors, subject to approval by the Contracting Officer) to retain, store and transmit any Customer information and data, subject to Government security requirements that Customer discloses to Proofpoint and pursuant to the normal functioning of Proofpoint Products. Customer information and data includes, but is not limited to (i) all configuration, rules and policies executed at Customer's direction; (ii) any document management or retention protocols that would delete, track, transmit or route documents or other data; (iii) any requests by Customer or required hereunder for log, access, support-related or other transmissions under this Agreement.

5. Data Security & Privacy

5.1 Limited Use of Personal Data. Proofpoint and its subsidiaries are authorized to access and process Personal Data solely in accordance with the terms of the Agreement. Proofpoint and its subsidiaries shall take reasonable steps to ensure the reliability of any employee, agent or subcontractor who may have access to the Personal Data and will ensure access is strictly limited to those individuals who need to access the relevant Personal Data in the performance of Proofpoint's obligations under the Agreement.

5.2 Data Safeguards. Proofpoint will maintain reasonable administrative, physical, and technical safeguards for protection of the security and confidentiality of Customer Data and Personal Data, including, but not be limited to, measures for preventing unauthorized access, use, modification or disclosure of Customer Data and Personal Data. When processing any Customer Data and Personal Data, Proofpoint will comply with its Data Security, Protection, Audit and Compliance Policy at https://www.proofpoint.com/us/legal/license which is incorporated by reference in full and made a part hereof.

5.3 "Customer Data" means the Customer specific configurations and rules implemented in the Proofpoint Products, and any Customer content processed by the Proofpoint Products (e.g., email text and attachments) that is not Personal Data. "Personal Data" means data about an identifiable individual that is protected by privacy laws where the individual resides. Examples of personal data include name, religion, gender, financial information, national identifier numbers, health information, email addresses, IP addresses, online identifiers and location data.

5.4 Proofpoint Products in FedRAMP. When Proofpoint delivers designated Government Proofpoint Products, notwithstanding anything contained in this license agreement to the contrary, the Proofpoint FedRAMP System Security Plan (SSP) on file with the FedRAMP Program Management Office (PMO) shall govern exclusively all data security obligations solely with respect to such Government Proofpoint Products.

6. Confidentiality

6.1 Receiving Party shall not (i) disclose any Confidential Information of the Disclosing Party to any third party, except as otherwise expressly permitted herein, or (ii) use any Confidential Information of Disclosing Party for any purpose outside the scope of the Agreement, except with Disclosing Party's prior written consent. The Receiving Party shall not make Confidential Information available to any of its employees or consultants except those that have agreed to obligations of confidentiality at least as restrictive as those set forth herein and have a "need to know" such Confidential Information. The Receiving Party agrees to hold the Disclosing Party's Confidential Information in confidence and to take all precautions to protect such Confidential Information that the Receiving Party employs with respect to its own Confidential Information of a like nature, but in no case shall the Receiving Party employ less than reasonable precautions. The Agreement will not be construed to prohibit disclosure of Confidential Information to the extent that such disclosure is required to by law or valid order of a court or other governmental authority; provided, however, to the extent permitted by law, the responding party shall give prompt written notice to the other party to enable the other party to seek a protective order or otherwise prevent or restrict such disclosure and, if disclosed, the scope of such disclosure is limited to the extent possible. When the end user is the Federal Government, neither this Agreement nor the pricing terms are confidential information notwithstanding any such markings.

6.2 The Receiving Party will return all copies of the Disclosing Party's Confidential Information upon the earlier of (i) the Disclosing Party's request, or (ii) the termination or expiration of the Agreement. Instead of returning such Confidential Information, the Receiving Party may destroy all copies of such Confidential Information in its possession; provided, however, the Receiving Party may retain a copy of any Confidential Information disclosed to it solely for archival purposes, provided that such copy is retained in secure storage

and held in the strictest confidence for so long as the Confidential Information remains in the possession of the Receiving Party.

6.3 The parties acknowledge and agree that the confidentiality obligations set forth in this Master Agreement are reasonable and necessary for the protection of the parties' business interests, that irreparable injury may result if such obligations are breached, and that, in the event of any actual or potential breach of this Confidentiality provision, the non-breaching party may have no adequate remedy at law and shall be entitled to seek injunctive and/or other equitable relief as may be deemed proper by a court of competent jurisdiction in accordance with Federal law.

6.4 Subject to the Freedom of Information Act and applicable Federal law, "Confidential Information" means all confidential and proprietary information of a party ("Disclosing Party") disclosed to the other party ("Receiving Party"), whether orally or in writing, that is designated as "confidential" or the like, or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure the Proofpoint Products business and marketing plans, technology and technical information, product designs, and business processes. "Confidential Information" shall not include information that (i) is or becomes a matter of public knowledge through no act or omission of the Receiving Party; (ii) was in the Receiving Party's lawful possession prior to the disclosure without restriction on disclosure; (iii) is lawfully disclosed to the Receiving Party by a third party that lawfully and rightfully possesses such information without restriction on disclosure; (iv) the Receiving Party can document resulted from its own research and development, independent of receipt of the disclosure from the Disclosing Party; or (v) is disclosed with the prior written approval of the Disclosing Party.

7. Support and Service Levels.

7.1 Support Services. Proofpoint shall provide support and/or Managed Services to the extent provided in a purchase order. Proofpoint's current support terms are attached hereto and made a part hereof as Exhibit 1 and represents what is currently found at https://www.proofpoint.com/us/legal/license.

7.2 Service Levels. Proofpoint provides a Service Level Agreement ("SLA") for the applicable Proofpoint Service. The applicable product SLAs are attached hereto and made a part hereof as Exhibit 2 and represent what is currently found at https://www.proofpoint.com/us/legal/license. In the event of a breach of an SLA, as Customer's sole and exclusive remedy, Proofpoint shall provide the remedy set forth in the applicable SLA.

8. Reporting and Audit. Customer shall monitor and report its actual usage of the subscription-based Proofpoint Products ("License Count"). A "Base License" is the number of Licenses for which Customer has paid Subscription Fees. Customer will provide Proofpoint with a License Count on or before the date on which the then-current License Count exceeds the Base License Count by ten percent (10%) or more (if applicable) by email at accountsreceivable@proofpoint.com. Proofpoint may also at any time produce an actual license count for verification by Customer. If, in either case, the License Count is greater than the Base License, Proofpoint will promptly invoice Customer additional license fees for each License beyond the Base License from the time such Licenses were activated through the remainder of the Initial Term or Extension Term, as applicable, in accordance with the provision below.

Additional License Count Invoice.

Discrepancies found in an audit may result in a charge by Proofpoint to the ordering activity through the Contractor. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order. This charge, if disputed by the ordering activity, will be resolved in accordance with the FAR or applicable FAR supplement Disputes clause. No payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process. Any audit requested by Proofpoint will be performed at Proofpoint's expense, without reimbursement by the Government. Undisputed fees shall be paid in accordance with this Agreement.

9. Warranty

9.1 Warranties and Remedies.

(a) *Performance Warranties*. Proofpoint warrants that during the Subscription Term the applicable Service ("SaaS Warranty") and Software ("Software Warranty") will substantially conform in all material respects to the Documentation. Customer will provide prompt written notice of any non-conformity. Proofpoint may modify the Documentation in its sole discretion, provided the overall level of the Service or Software, as applicable, will not decrease during the Term. The Software Warranty does not apply to: (a) Software that has been modified by any party other than Proofpoint; or (b) Software that has been improperly installed or used in a manner other than as authorized under the Agreement.

(b) *SaaS and Software Warranty Remedy*. As Customer's sole and exclusive remedy and Proofpoint's entire liability for any breach of the SaaS Warranty or the Software Warranty, Proofpoint will (a) use reasonable efforts to fix, provide a work around, or otherwise repair or replace the Service or Software, as applicable, or if Proofpoint is unable to do so, (b) terminate the license to use such component of the Service or the applicable Software and return the Subscription Fees paid to Proofpoint for such allegedly defective Service or Software, as applicable, for the period commencing from Customer's notice of nonconformity through the remainder of the Initial Term or Extension Term, as applicable.

9.2 Warranty Disclaimers.

EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH ABOVE, PROOFPOINT AND PROOFPOINT LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AS WELL AS ANY WARRANTIES OF REGULATORY COMPLIANCE, PERFORMANCE, ACCURACY, RELIABILITY, AND NONINFRINGEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT.

PROOFPOINT DOES NOT WARRANT: (I) THE ACCURACY OF THE INTENDED EMAIL BLOCKING OF ANY MAIL MESSAGE; (II) THAT EMAIL WILL NOT BE LOST; (III) THAT THE OPERATION OF THE PROOFPOINT PRODUCTS WILL BE UNINTERRUPTED OR ERROR-FREE; (IV) THAT ALL SOFTWARE ERRORS WILL BE CORRECTED; OR (V) THAT THE PROOFPOINT PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS OR ATTACKS.

10. Limitation of Liability. The limitation of liability set forth herein shall not apply to (1) personal injury or death resulting from Licensor's negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law. All consequential, incidental, special, punitive, exemplary, and indirect damages (including lost profits and loss of data) are disclaimed on behalf of Proofpoint (and Proofpoint is also required under its contracts with its suppliers and licensors to state in this Agreement that such suppliers and licensors also disclaim such damages herein). The foregoing exclusions/limitations of liability shall not apply (1) to personal injury or death caused by Proofpoint's negligence or fraud; (2) for express remedies requiring the specific type of relief under the law or these license terms; or (3) for any other matter for which liability cannot be excluded by law.

EXCEPT FOR (i) INTELLECTUAL PROPERTY INDEMNIFICATION OBLIGATIONS HEREIN, (ii) DAMAGES RESULTING FROM EITHER PARTY'S GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT, (iii) DAMAGES RESULTING FROM EITHER PARTY'S MATERIAL BREACH OF THE CONFIDENTIALITY SECTION, (iv) CUSTOMER'S BREACH OF THE CUSTOMER RESPONSIBILITIES SECTION, EACH PARTY'S AGGREGATE LIABILITY UNDER THE AGREEMENT FOR ANY CLAIMS, DAMAGES, OR LIABILITIES ("CLAIMS") SHALL IN NO EVENT EXCEED THE SUBSCRIPTION FEES PAID FOR THE APPLICABLE PROOFPOINT PRODUCT OVER THE PRECEDING TWELVE MONTHS FROM WHEN SUCH CLAIM AROSE.

THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733. FURTHERMORE, THIS CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT'S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE GSA SCHEDULE CONTRACT (E.G., GSAR CLAUSE 552.238-81 – PRICE REDUCTIONS, AND CLAUSE 552.215-72 – PRICE ADJUSTMENT – FAILURE TO PROVIDE ACCURATE INFORMATION).

11. Intellectual Property Rights.

11.1 Ownership. Customer retains all title, intellectual property and other ownership rights in all Customer Confidential Information, Customer Data and all data that Customer makes available for processing by the Proofpoint Products. Proofpoint retains all title, intellectual property and other ownership rights throughout the world in and to the Proofpoint Products, Documentation, and any work product and any modifications to, and derivative works of, the foregoing. Proofpoint hereby grants to Customer a non-exclusive, non-transferable, fully paid-up license to use any work product in connection with the Proofpoint Product licensed under the Agreement and solely for Customer's internal business purposes.

11.2 No Implied Rights. There are no implied rights and all rights not expressly granted herein are reserved. No license, right or interest in any Proofpoint trademark, copyright, patent, trade name or service mark is granted

hereunder. Customer shall not remove from any full or partial copies made by Customer of the Software, Software Updates and Documentation any copyright or other proprietary notice contained in or on the original, as delivered to Customer.

11.3 Proofpoint Authorization and License. During the Term of the Agreement, Customer hereby (i) grants to Proofpoint and its service providers a worldwide, limited term license to collect and process certain Customer Confidential Information and Customer Data, and (ii) authorizes Proofpoint to collect and process certain Personal Data, for: (a) abuse, fraud and threat awareness, detection and prevention, (b) compliance, and (c) security purposes, in accordance with the Agreement. "Customer Data" means the Customer specific configurations and rules implemented in the Proofpoint Products, and any Customer content processed by the Proofpoint Products (e.g., email text and attachments) that is not Personal Data.

Customer acknowledges and agrees that development of Threat Analytics from Proofpoint's ecosystem is critical to the functionality of the Proofpoint Products. Customer hereby authorizes Proofpoint to collect Threat Analytics during the Term of the Agreement. Further, Customer hereby authorizes Proofpoint to use Threat Analytics worldwide to build, enhance, improve and maintain Proofpoint services; provided that if Customer provides written legal notice to Proofpoint on or after expiration or termination of the applicable Proofpoint Services instructing Proofpoint to delete any Personal Data included in Threat Analytics, it will be deleted within 18 months of such notice. "Threat Analytics" means information collected, generated and/or analyzed by the Proofpoint Products such as log files, statistics, aggregated data and derivatives thereof.

12. Intellectual Property Rights Indemnification.

12.1 Proofpoint's Duty to Indemnify. Subject to the subsections below within this section, Proofpoint agrees to defend and indemnify Customer from and against any third-party claim filed against Customer alleging that the Proofpoint Product(s), as sold and delivered to Customer (the "Indemnified Products"), directly infringe the valid intellectual property rights of a third party (an "IP Claim"). Proofpoint agrees to pay and hold Customer harmless against any amounts finally awarded by a court having competent jurisdiction in respect of such IP Claim or pursuant to a settlement accepted by Proofpoint in writing. Proofpoint may, at its sole election and expense: (i) procure sufficient rights to allow Customer continued use of the Indemnified Products under the terms of the Agreement; (ii) replace or modify the Indemnified Products to avoid the alleged infringement; or (iii) if the foregoing options are not reasonably practicable, terminate Customer's rights to use the Indemnified Products and refund all amounts paid by Customer to Proofpoint attributable to Customers' future usage or access to the Indemnified Products. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

12.2 Exclusions. Proofpoint shall have no obligation or any liability to Customer for any IP Claim arising out of or related to: (i) modifications or adaptations to the Indemnified Products made by Customer or Customer's agents; (ii) the use of the Indemnified Products in combination with any other product, service or device, if the IP Claim would have been avoided by the use of the Indemnified Products without such other product, service or device not provided by Proofpoint to Customer or Customer's agents; (iii) compliance with Customer's specific instructions for customization of an Indemnified Product made solely for or on behalf of Customer; (iv) use or exploitation of the Indemnified Products other than as set forth in the Agreement or applicable Documentation; or (v) Customer being given an update, modification, or replacement to an Indemnified Product by Proofpoint and failing to implement such update, modification, or replacement within a reasonable period of time.

12.3 Process. Proofpoint's obligations under this section are conditioned upon the following: (i) Customer first providing written notice of the IP Claim to Proofpoint within thirty (30) days after Customer becomes aware of or reasonably should have been aware of the IP Claim (provided, however, the failure to provide such notice will only relieve Proofpoint of its indemnity obligations hereunder to the extent Proofpoint is prejudiced thereby); (ii) Customer tendering control of the IP Claim to Proofpoint at the time Customer provides written notice of such IP Claim to Proofpoint; provided that, the US Department of Justice has the sole right to represent the United States in any action, in accordance with 28 U.S.C. 516; and (iii) Customer providing reasonable assistance, cooperation and required information with respect to defense and/or settlement of the IP Claim. Customer may at its sole expense participate in the IP Claim defense, except that Proofpoint will retain control of the defense and/or settlement, to the extent consistent with Federal law. Proofpoint shall not agree to any settlement of an IP Claim that includes an injunction against Customer or admits Customer liability without Customer's prior written consent.

12.4 Exclusive Remedy. This section describes the sole and exclusive remedy of Customer and the entire liability of Proofpoint with respect to any IP Claim.

13. **Termination.** On termination or expiration of the Agreement, all Software licenses, Service access, granted

under the Agreement shall automatically terminate with immediate effect. In the event of the termination or expiration of the Agreement, the provisions of the Agreement which by their nature extend beyond the expiration or termination of the Agreement shall survive. Within thirty (30) days after expiration or termination of the License to use the Proofpoint Product, Customer shall: (i) certify in writing to Proofpoint that all copies of the Software, Software Updates, and Documentation in any form, including partial copies or extracts thereof, have been destroyed or returned to Proofpoint, and (ii) retrieve or dispose of Customer data from or within the Proofpoint Products and/or systems. Upon 30 days of termination of the License to use the Proofpoint Product, Customer data in the Proofpoint Product and/or systems may be rendered illegible, deleted or written over, including any back-up Customer data.

14. Miscellaneous.

A. Law. This Agreement shall be governed by the federal law of the United States. The Uniform Computer Information Transaction Act shall not apply to this Agreement.

B. Force Majeure. Excusable delays shall be governed by FAR 52.212-4(f).

C. Entire Agreement. This Agreement constitutes the entire agreement of the parties and supersedes all prior or contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No amendment or waiver of any provision of the Agreement shall be effective unless in writing and signed by the party against whom the amendment or waiver is to be asserted.

D. Severability. If any clause of the Agreement shall be adjudged by any board, court or tribunal of competent jurisdiction to be invalid or unenforceable, such judgment shall not affect, impair or invalidate the remainder of the Agreement, which shall remain enforceable by the parties. For the avoidance of doubt, with respect to any Federal prime contract, subcontract, or end-user licensing agreement which incorporates Proofpoint's terms and conditions, those clauses that are specifically declared by Federal regulation not to be enforceable, shall be deemed deleted from the Agreement to the extent they are determined to be unenforceable.

E. Taxes. Any taxes charged to Proofpoint shall be invoiced to prime contractor for payment by the Government subject to the following. Any such taxes invoiced will be governed by the terms of the underlying Government prime contract or order between the prime contractor and the Government and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government prime contract. Proofpoint shall state separately on invoices taxes excluded from the fees, and the Government agrees either to pay the amount of the taxes or provide evidence necessary to sustain an exemption, in accordance with FAR 52.229-1 and FAR 52.229-3.

F. Open Source Software: Proofpoint Appliance/Software for Customer On-Site Deployment. Open Source Software may be a component of the Software provided to Customer for on-site deployment. Proofpoint is required by Open Source Software requirements to inform the end user of certain facts, including the following:

"Open Source Software" means various open source software, including GPL software which is software licensed under the GNU General Public License as published by the Free Software Foundation, and components licensed under the terms of applicable open source license agreements included in the materials relating to such software. Open Source Software is composed of individual software components, each of which has its own copyright and its own applicable license conditions. Customer may obtain information (including, if applicable, the source code) regarding the inclusion of Open Source Software in the Software by sending a request, with Customer's name and address to Proofpoint at the address specified in the Order. Customer may redistribute and/or modify the GPL software under the terms of the GPL. A copy of the GPL is included on the media on which Customer receives the Software or included in the files if the Software is electronically downloaded by Customer. This offer to obtain a copy of the source files for GPL software is valid for three (3) years from the date Customer acquired the Appliance Software. By executing this agreement, Customer does not agree to be bound by any Open Source terms without executing an agreement in writing. Customer acknowledges that third party software has different terms.

Exhibit 1

Support Services

SUPPORT SERVICES PROGRAM FOR PROOFPOINT CUSTOMERS

Overview: The support services described herein are provided by Proofpoint to each Proofpoint customer ("Customer") pursuant to the terms and conditions of the applicable license agreement ("Agreement") between each customer and Proofpoint or between a customer and an authorized Proofpoint partner. Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. Subject to customer paying the applicable support related fees, Proofpoint will provide the support described herein.

1. Software and Documentation Updates. Regardless of support level purchased by Customer, Proofpoint shall provide to Customer one (1) electronic copy of all updated revisions to the Documentation and one (1) electronic copy of generally released bug fixes, maintenance releases and updates of the Software (collectively, "Updates"). Updates do not include products or options that are designated by Proofpoint as new products or options for which Proofpoint charges a separate fee. Software releases are supported for the current and prior release that are designated by a change to the right of the decimal point (e.g., 1.1 to 1.2) or as stated in the support schedule posted on Proofpoint's Support Portal (found at www.proofpoint.com/community). Prior to discontinuing support services for any Software product line, Proofpoint shall provide at least six (6) months advance notice on its support website.

1.1 Support Service Levels. Proofpoint offers three support levels: Self-Service Support, Platinum Support, and Premium Support. Customers with Platinum Support or Premium Support also have the ability to purchase the optional Global Add-On.

1.1.1 Self-Service Support. For Self-Service Support, Customer shall receive two (2) Authorized Support Contacts. Phone support is available only for Priority 1 program issues (described in Section 2.1 below) and only during Proofpoint business hours. For all other program issue priority levels Proofpoint shall use commercially reasonable efforts to correct and/or provide a work-around for any issue reported by Customer in the current unmodified release of the Software in accordance with the priority level reasonably assigned to such issue by Customer. 24x7 support is not available for Self-Service Support customers.

1.1.2 Platinum Support. In addition to Self-Service Support, for an additional charge, Customer shall receive (i) assistance for Priority I issues, as reasonably determined by Proofpoint, 24x7, 365 days per year and (ii) access to support phone lines. Handling of non-Priority I issues will take place during the support hours specified in Section 1.2.

1.1.3 Premium Support. In addition to Self-Service Support and Platinum Support, as defined above, for an additional charge, Customer shall receive (i) access to support phone lines and (ii) Proofpoint will assign a designated Technical Account Manager to Customer's account.

1.1.4 Global Time Zone Add On. Any Customer that has purchased support at Platinum Support level or higher, may purchase the Global Time Zone Add On. For an additional charge, Proofpoint shall provide assistance for issues of any priority, as reasonably determined by Proofpoint, 24x7, 365 days per year.

1.2 Support Requests and Authorized Support Contacts. Technical support is available during the technical support hours for the primary support center specified on the Product Order Form. Technical support hours for the Americas are Monday through Friday, 12:00 UTC to 03:00 UTC the following day (e.g. 07:00am EST to 10:00pm EST during standard time and excluding Proofpoint holidays). Technical support hours for Europe are Monday through Friday, 04:00 UTC to 19:00 UTC (e.g. 05:00am CET to 08:00pm CET during standard time and excluding Proofpoint holidays). Technical support hours for Asia Pacific are Sunday through Thursday 21:00 UTC to 12:00 UTC (e.g. Monday through Friday 06:00am JST to 09:00pm JST during standard time and excluding Proofpoint holidays). Technical support hours for the Middle East are Saturday through Thursday 03:00 UTC to 15:00 UTC (e.g. 07:00am GST to 07:00pm GST during standard time and excluding Proofpoint holidays). Customer may initiate electronic support requests through Proofpoint's web-based portal (the "Proofpoint Communities") at any time. Support requests submitted via the Proofpoint Communities will be addressed by Proofpoint during the support hours listed above. Customer will promptly identify two internal resources who are knowledgeable about Customer's operating environment and operation of the Proofpoint Products (collectively, "Authorized Support Contacts"). Authorized Support Contacts will serve as primary contacts between Customer and Proofpoint and are the only persons

authorized to interact with Proofpoint Technical Support, including accessing the Proofpoint Support Services Program Rev 3-2021 Proofpoint Communities to submit and track cases. All support requests will be tracked in the Proofpoint Communities and Customer can view the status of Customer's cases on the Proofpoint Communities at any time.

1.3 Authorized Support Contact Training. It is highly recommended that Authorized support contacts take the authorized support contact training available in Proofpoint's training platform, LevelUp! This training covers best practices for working with Proofpoint support, including how to create a support ticket, using the Proofpoint community, troubleshooting best practices.

2. Priority Levels of Issues and Targeted Responses In the performance of support services, Proofpoint will apply the following priority ratings and targeted response times to Platinum Support and Premium Support.

2.1 Priority I Issues

A "Priority I Issue" means a Software program issue which both (i) prevents some critical function or process from substantially meeting the Documentation and (ii) seriously degrades the overall performance of such function or process such that no useful work can be done and/or some primary major function of the Software or Appliance is disabled. Priority I Issues shall receive an initial response within one (1) hour (during standard support hours referenced above), of the case being submitted to Proofpoint. In addressing a Priority I Issue, Proofpoint shall use all reasonable efforts to develop a suitable workaround, patch, or other temporary correction to restore operation as soon as possible. Proofpoint efforts to resolve a Priority 1 Issue will include the following: (1) assigning one or more senior Proofpoint engineers on a dedicated basis to develop suitable workaround, patch, or other temporary correction; (2) notifying senior Proofpoint management that such P1 Issue has been reported; (3) providing Customer with periodic reports on the status of corrections; and (4) providing a final solution to Customer as soon as it is available.

2.2 Priority II Issues

A "Priority II Issue" means a Software program issue which both (i) degrades some critical function or process from substantially meeting the Documentation and (ii) degrades the overall performance of such function or process such that useful work is hindered and/or some major function of the Software or Appliance is not operating as expected but can be worked- around. Priority II Issues shall receive an initial response within four (4) hours (during standard support hours referenced above). Proofpoint shall use all reasonable efforts to provide a workaround, patch, or other temporary correction as soon as possible.

2.3 Priority III Issues.

A "Priority III Issue" means a Software program issue which both (i) prevents some non-essential function or process from substantially meeting the Documentation and (ii) significantly degrades the overall performance of the Software or Appliance. Priority III Issues shall receive an initial response within eight (8) hours (during standard support hours referenced above). Proofpoint shall use all reasonable efforts to provide a workaround, patch, or other temporary correction as soon as possible.

2.4 Priority IV Issues

A "Priority IV Issue" means a Software program issue which prevents some function or process from substantially meeting the Documentation but does not significantly degrade the overall performance of the Software or Appliance. Priority IV Issues shall receive an initial response within sixteen (16) hours (during standard Support hours referenced above). Proofpoint shall use all reasonable efforts to include a workaround, patch, or other temporary correction in the next Software update.

3. Customer Cooperation and Proofpoint's License.

3.1 Customer Cooperation. Proofpoint's obligation to provide support services is conditioned upon the following: (i) Customer's reasonable effort to resolve the problem after communication with Proofpoint; (ii) Customer's provision to Proofpoint of sufficient information and resources to correct the problem, including, without limitation, remote access as further discussed in these policies, (iii) Customer's prompt installation of all Software maintenance releases, bug fixes and/or work-around supplied by Proofpoint, and (iv) Customer's procurement and installation

and maintenance of all hardware necessary to operate the Software. As related to Priority I Issues, Customer shall provide continuous access to appropriate Customer personnel and the Appliance (if applicable) during Proofpoint's response related to the Priority I Issue or Proofpoint shall be permitted to change the Priority of the issue.

3.2 Proofpoint's License. During the term of the support services and for purposes relating to providing support to Customer, Proofpoint may obtain information regarding Customer's e-mail communications, and Customer agrees that Proofpoint may use any statistical data generated relating to Customer's e-mail. Customer hereby grants to Proofpoint and its service providers a worldwide, limited term license to collect and process certain Customer Confidential Information, Customer Data and Personal Data for: (a) abuse and threat awareness, detection and prevention, (b) compliance, and (c) security purposes in accordance with the Agreement. Customer acknowledges and agrees that development of Threat Analytics from Proofpoint's ecosystem is critical to the functionality of the Proofpoint Products. Customer hereby grants a worldwide license to Proofpoint to collect Threat Analytics during the Term of the Agreement. Further, Customer hereby grants a worldwide license to Proofpoint to use Threat Analytics to maintain, improve and enhance Proofpoint services; provided that if Customer provides written legal notice to Proofpoint on or after expiration or termination of the applicable Proofpoint Services instructing Proofpoint to delete any Personal Data included in Threat Analytics it will be deleted within 18 months of such notice. Notwithstanding the foregoing, Proofpoint shall not disclose the source and content of any such e-mail. This Section 3.2 survives termination and expiration of the Agreement.

4. Reproducing Problems; Remote Access.
Subject to the applicable support services fees, support services assistance is limited to Software on platforms that are fully supported, running unaltered on the proper hardware configuration. Where applicable for a reported issue, Proofpoint will use commercially reasonable efforts to reproduce the problem so that the results can be analyzed. Proofpoint's obligation to provide the support services described herein, including without limitation meeting the response times set forth in Section 2 above, is subject to Customer providing shell or Web-based remote access to Customer's computer system(s) and network. Any such remote access by Proofpoint shall be subject to Proofpoint's compliance with Customer's security and antivirus procedures and the confidentiality requirements set forth in the license agreement between Proofpoint and Customer. Any delay occasioned by Customer's failure to provide the foregoing remote access shall extend the response time periods set forth in Section 2 accordingly and resolution of the problem may be subject to payment of additional fees. Prior to proceeding with work that will be subject to additional fees, Proofpoint will notify Customer and will not start such work until Proofpoint receives authorization from Customer. If Customer fails to provide remote access to its computer system(s) and network and Proofpoint and Proofpoint and Customer cannot agree on a mutually satisfactory alternative method of reproducing the problem, Proofpoint shall not be obligated to resolve the problem.

5. Support Services Conditions.
5.1 Support Issues Not Attributable to Proofpoint. Proofpoint is not obligated to provide support services for problems related to: (i) unauthorized modifications and/or alterations of the Software, (ii) improper installation of the Software by non-Proofpoint personnel, use of the Software on a platform or hardware configuration other than those specified in the Documentation or in manner not specified in the Documentation, or (iii) problems caused by the Customer's negligence, hardware malfunction, or third-party software. In the event Proofpoint provides support services for problems caused by any of the above, Customer will reimburse Proofpoint for such services at the then-current time and materials rate. Proofpoint shall be entitled to discontinue support services in the event of Customer's non-payment of Subscription Fees when due.

5.2 Exclusions from Support services.
The following items are excluded from support services:
(a) In-depth training. If the support request is deemed to be training in nature, and will require an extended amount of time, Customer will be referred to Proofpoint's training or consulting departments.
(b). Assistance in the customization of the application. Support services do not include providing assistance in developing, debugging, testing or any other application customization
(c). Information and assistance on third party products. Issues related to the installation, administration, and use of enabling technologies such as databases, computer networks, and communications (except an Appliance) are not provided under Proofpoint support services.
(d) Assistance in the identification of defects in user environment. If Proofpoint concludes that a problem being reported by a Customer is due to defects in Customer's environment, Proofpoint will notify the Customer. Additional support by Proofpoint personnel to remedy performance issues due to the user environment are categorized as consulting services, which are provided for an additional fee.
(e). Installation. Support Services provided herein do not include the use of Proofpoint support services resources to

perform installation of updates or Customer-specific fixes. If Customer wishes to have Proofpoint perform services related to any of the above items, such services will be performed pursuant to a mutually executed SOW.

6. Description of Appliance Support Services.

6.1 Services.

For as long as the Appliance purchased by Customer is under Proofpoint's Appliance warranty Customer shall contact Proofpoint for any and all maintenance and support related to the Appliance. If support for the Appliance purchased by Customer includes on-site support, Proofpoint shall provide or cause to be provided 8-hour response service during the support hours specified in Section 1.2. A technician will arrive on-site, depending on Customer's location and the availability of necessary parts, as soon as practicable (within the business hours specified in Section 1.2) after problem determination. Optional 24x7 service is available subject to Section 1.1.4.

6.2 Customer Obligations.

Customer must also install remedial replacement parts, patches, software updates or subsequent releases as directed by Proofpoint in order to keep Customer's Appliance eligible for support services. Customer agrees to give Proofpoint at least thirty (30) days written notice prior to relocating Appliance. It is Customer's responsibility to back up the data on Customer's system, and to provide adequate security for Customer's system. Proofpoint shall not be responsible for loss of or damage to data or loss of use of any of Customer's computer or network systems. Customer agrees to provide the personnel of Proofpoint or its designee with sufficient, free, and safe access to Customer's facilities necessary for Proofpoint to fulfill its obligations.

6.3 Exclusions.

Appliance support services do not cover parts such as batteries, frames, and covers or service of equipment damaged by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by Customer, removal or alteration of equipment or parts identification labels, or failure caused by a product for which Proofpoint is not responsible.

Exhibit 2
Service Level Agreements

Hosted Services Service Level Agreement

1. Standard Terms Applicable to each SLA:

A. **Definitions.** Except as otherwise modified or defined herein, all capitalized terms in this Hosted Services Service Level Agreement have the same meanings as set forth in the General Terms and Conditions and the applicable Product Exhibit (collectively, "Agreement"). For purposes of this Hosted Services Service Level Agreement the following definitions will apply.

A.1 **"**Scheduled Maintenance Window" means the window during which weekly scheduled maintenance of the Hosted Service may be performed. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.

A.2 "Emergency Maintenance" means any time outside of Scheduled Maintenance Window that Proofpoint is required to apply urgent patches or fixes, or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the Hosted Service to be unavailable during the Emergency Maintenance.

B. Service Credits

B.1 "Service Credit" means the percentage of the monthly Subscription Fees paid or payable for the Hosted Service product that is awarded to Customer for a validated claim associated with that portion of the Hosted Service related to breach of the applicable SLA during that month.

B.2 In any given month Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming Hosted Service product.

B.3 Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Hosted Service product subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied against amounts due for an Extension Term. If Service Credits cannot be applied to future Subscription Fees because the Agreement has terminated due to Proofpoint's breach of the Agreement, Proofpoint will promptly pay Customer the amount of the Services Credit.

C. SLA Claims

C.1 Customer must notify Proofpoint Customer Support via support ticket within five (5) business days from the occurrence of the SLA incident. Customer's claim ticket must identify which specific SLA applies and the details of the relevant incident. Distributors and channel partners may NOT open SLA tickets on behalf of a Customer. If requested by Proofpoint Customer will provide Proofpoint a live copy of the applicable email with the original Proofpoint headers (complete and untampered with) for analysis. Failure to comply with these reporting requirements may forfeit Customer's right to receive a remedy in connection with an SLA.

C.2 For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. Proofpoint shall make information used to validate a SLA claim available for auditing by Customer at Customer's request.

C.3 In the event that more than one aspect of a Hosted Service product is affected by the same root cause, the single SLA applicable to such Hosted Service product of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

C.4 Except for gross negligence or willful misconduct, the remedies set forth herein represents Customer's sole and exclusive remedy for Proofpoint's breach of the SLAs defined in this SLA.

D. Exclusions

D.1 Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of the Hosted Service product outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Proofpoint's data center and not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; or (iv) a Force Majeure Event. These SLAs do not apply to any end of life product or software version.

2. SECURITY SERVICES HOSTED SERVICE SLAs. The following SLAs apply to the Security Services Hosted Service.

A. Filtering System Availability SLA.

A.1 Proofpoint warrants at least 99.999% System Availability, which is defined as % of total time during which email service connectivity on port 25 is available during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance. For purposes of calculating System Availability, only downtime occurrences exceeding 30 seconds will apply.

A.2 **Customer Responsibilities.** Customer must: (a) set up MX records and outbound entries in accordance with the Hosted Service product latest welcome letter provided to Customer; (b) identify the number of impacted users as a subset against the total number of licensed users; (c) if inbound email is impacted provide the timeframes of the Service unavailability; (d) if outbound email is impacted provide copies of impacted email with the original Proofpoint headers complete and unaltered; and (e) provide ping and trace routes.

A.3 **Remedy.** If the email System Availability is less than 99.999%, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet the email System Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of Email System Availability per Calendar Month	Service Credit
< 99.999%	25%
< 99. 0%	50%
< 98.0%	100%

B. Email Delivery SLA

B.1 Proofpoint warrants that the average of Email Delivery (as defined below) times, as measured in minutes over a calendar month, will be one (1) minute or less.

B.2 For purposes of this SLA "Email Delivery" is defined as the elapsed time from when a business email enters the Security Services Hosted Service network to when it exits the Security Services Hosted Service network. The Email Delivery average time measurement for a cluster is calculated using simulated or test emails. These test emails are sent at a periodic frequency and the fastest 95% email delivery times are tracked by Proofpoint to calculate the average for that month.

B.3 This SLA applies only to legitimate business email (e.g. not to non-solicited bulk email) delivered to valid Mailbox accounts that are contracted for the Security Services Hosted Service.

B.4 **Exclusions**. Customer shall not have any remedies under this SLA to the extent any SLA claim hereunder is due to (i) delivery of email to quarantine; (ii) email in deferral queues; (iii) email loops; (iv) attachments (only if Customer holds a license to Targeted Attack Protection Attachment Defense); (v) suspect spam; (vi) zero hour wait; or (vii) Customer's primary email server is unable to accept email on initial attempt.

B.5 **Remedy.** If in any calendar month the Email Delivery SLA is not met and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

Average Email Delivery Time	Service Credit
> 1 minute	25%
> 5 minutes	50%
> 10 minutes	100%

C. Virus Filtering SLA

C.1 Proofpoint warrants that the Security Services Hosted Service will Filter (as defined below) 100% of all Viruses (as defined below) contained in an inbound email to a Customer Mailbox for which a Security Services Hosted Service subscription has been purchased**.**

C.1.1 Proofpoint warrants that the Security Services Hosted Service will Filter 100% of all Viruses contained in an outbound email from a Customer Mailbox for which a Security Services Hosted Service subscription has been purchased**.**

C.2 For purposes of this SLA, the following definitions shall apply:

C.2.1 "Filter" means to detect and block or quarantine all email messages with Viruses that:

(i) match an available virus signature generally available from Customer's selected and licensed anti-virus engine vendor; and

(ii) are identifiable by industry standard anti-virus engine heuristics; and

(iii) are propagated through registered attachment types that are recognized by Customer's selected and licensed anti-virus engine vendor.

C.2.2 "Infection" means if an inbound email to a Customer Mailbox is delivered with a Virus, or if an outbound email from a Customer Mailbox is processed through the Security Services Hosted Service with a Virus without being quarantined.

C.2.3 "Virus" means a binary or executable code whose purpose is to gather information from the infected host (such as trojans), change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources.

C.3 This SLA does not apply to (i) text messages that use fraudulent claims to deceive the Customer and/or prompt the Customer to action (such as phishing); (ii) a binary or executable code installed or run by an end user that gathers information for sales and marketing purposes (such as spyware); (iii) a virus that has been detected and has been cleaned by other virus scanning products; (iv) an ineffective or inactive virus contained in a bounced email; (v) a Virus-infected email that is quarantined by the Hosted Services but is subsequently delivered to an end user or administrator by such end user or administrator; (vi) emails containing attachments that are password protected, encrypted or otherwise under an end user's control; (vii) any action by a Customer end user or administrator that results in deliberate self-infection; or (viii) any Infection occurring within the first thirty (30) minutes of the anti-virus engine vendor's new general release of a virus's applicable signature.

C.4 Customer will not be eligible to receive a remedy under this SLA if Customer (i) is not subscribing to all anti-virus Security Services Hosted Service modules for all Customer Mailboxes for which a Security Services Hosted Service subscription has been purchased; (ii) has not enabled full virus protection for all Customer Mailboxes for which a Security Services Hosted Service subscription has been purchased; (iii) does not provide Proofpoint with conclusive written evidence (including the full Virus attachment for each email experiencing the Infection) that the Virus was caused by an email that passed through the Security Services Hosted Service network; and (iv) emails exceeding the applicable anti-virus engine's maximum scanning size limit identified in the vendor'sdocumentation.

C.5 **Remedy.** If a validated Infection occurs in any calendar month, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

Number of validated infections that occurred during a month	Service Credit
1 to 3 Validated Occurrences	25%
4 or more Validated Occurrences	50%

D. Spam Inbound Effectiveness SLA

D.1 Proofpoint warrants that the Security Services Hosted Service will detect 99% of inbound spam in each calendar month.

D.2 This SLA does not apply to false negatives to invalid Mailboxes. Additionally, this SLA applies only to spam messages processed through Proofpoint's Security Services Hosted Services and does not apply to email sent from users or domains that have been safelisted or whitelisted by Customer within the Security Services Hosted Service.

D.3 Proofpoint will make a good faith estimation of the spam capture rate based on the regular and prompt submission tothe Security Services Hosted Service support center of all false negatives to report spam missed by Security Services Hosted Service.

D.4 Proofpoint will estimate the percentage of spam detected by the Security Services Hosted Service by dividing the number of spam emails identified by the Security Services Hosted Service as recorded in the Security Services Hosted Servicereport logs by all spam emails sent to Customer. Proofpoint will estimate all spam emails sent to Customer by adding the number of spam messages (false negatives) missed by the Security Services Hosted Service and reported to the Security Services Hosted Service support team to the number of spam emails detected by the Security Services Hosted Service.

D.5 **Remedy.** If the Security Services Hosted Service detects less than 99% of inbound spam in any calendar month, andif Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

If monthly average spam capture rate is	Service Credit
< 99%	25%
< 98%	50%
< 95%	100%

E. Spam Outbound Effectiveness SLA

E.1 Proofpoint warrants that the Security Services Hosted Service will detect 95% of outbound spam in each calendar month.

E.2 This SLA does not apply to false negatives to invalid Mailboxes. Additionally, this SLA applies only to spam messages processed through Proofpoint's Security Services Hosted Services and does not apply to email sent from users or domains that have been safelisted or whitelisted by Customer within the Security Services Hosted Service.

E.3 Proofpoint will make a good faith estimation of the spam capture rate based on the regular and prompt submission to the Security Services Hosted Service support center of all false negatives to report spam missed by Security Services Hosted Service.

E.4 Proofpoint will estimate the percentage of spam detected by the Security Services Hosted Service by dividing the number of outbound spam emails identified by the Security Services Hosted Service as recorded in the Security Services Hosted Service report logs by all outbound emails sent from the Customer through the Security Services Hosted Service. Proofpoint will calculate the total number of emails sent from the Customer through the Security Services Hosted Service in each calendarmonth.

E.5 **Remedy.** If the Security Services Hosted Service detects less than 95% of outbound spam in any calendar month, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

If monthly average spam capture rate is	Service Credit
< 95%	25%
< 93%	50%
< 90%	100%

F. False Positive SLA

F.1 Proofpoint warrants that the ratio of legitimate business email incorrectly identified as spam by the Security Services Hosted Service to all email (inbound and outbound) processed by the Security Services Hosted Service for Customer in any calendar month will not be greater than 1:350,000.

F.2 Proofpoint will make a good faith estimation of the false positive ratio based on evidence timely supplied by Customer.

F.3 This SLA does not apply to (i) bulk, personal, or pornographic email; (ii) emails containing a majority of non-English language content; or (iii) emails blocked by a policy rule, reputation filtering, or SMTP connection filtering

F.4 **Remedy.** If Proofpoint does not meet this SLA in any calendar month, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

False Positive Ratio in a Calendar Month	Service Credit
> 1:350,000	25%
> 1:50,000	50%
> 1:1,000	100%

G. Proofpoint Key Service ("PKS") System Availability SLA

G.1 Proofpoint warrants at least 99.999% PKS System Availability to Customer to access existing encryption keys (e.g. PKS shall not be unavailable more than 26 seconds per month) during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance). "System Availability" means the percentage of total time during which PKS is available to Customer, excluding Scheduled Maintenance Window and Emergency Maintenance."

G.2 **Remedy.** If PKS System Availability is less than 99.999%, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this PKS System Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of PKS System Availability per Calendar Month	Service Credit
< 99.999%	25%
< 99.0%	50%
< 98.0%	100%

3. PKS HOSTED SERVICE SLAs. The following SLAs apply if PKS is used in conjunction with the Security Appliance Software:

A. PKS System Availability SLA

A.1 Proofpoint warrants at least 99.999% PKS System Availability to Customer to access existing encryption keys (e.g. PKS shall not be unavailable more than 26 seconds per month) during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance). "System Availability" means the percentage of total time during which PKS is available to Customer, excluding Scheduled Maintenance Window and Emergency Maintenance.

A.2 **Remedy.** If PKS System Availability is less than 99.999%, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this PKS System Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of PKS System Availability per Calendar Month	Service Credit
< 99.999%	25%
< 99.0%	50%
< 98.0%	100%

4. EMAIL ARCHIVING HOSTED SERVICE SLAs. The following SLAs apply to the Email Archiving Hosted Service.

A. SYSTEM AVAILABILITY SLA

A.1 Proofpoint warrants at least 99.9% Email Archiving Hosted Service System Availability to Customer to access existing archived data (e.g. the Email Archiving Hosted Service shall not be unavailable more than 43 minutes per month) during each calendar month, excluding Scheduled Downtime and Emergency Maintenance). "System Availability" means the percentage oftotal time during which Email Archiving Hosted Service System is available to Customer, excluding Scheduled Maintenance Window and Emergency Maintenance.

A2. Remedy. If the Email Archiving Hosted Service System Availability is less than 99.9%, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of Email Archiving Hosted Service Availability per Calendar Month	Service Credit
< 99.9%	10%
< 99.0%	15%
< 95.0%	25%

B. SEARCH PERFORMANCE SLA

B.1 Provided Customer has purchased the Email Archiving Hosted Service real-time search option, Proofpoint warrants that the median of Email Archiving Hosted Service search requests executed within a given calendar month will occur within 20seconds or less.

B.2 For purposes of this SLA search time refers to the elapsed time from when the Email Archiving Hosted Service datacenter receives the search request to the time at which the Email Archiving Hosted Service is ready to return result information to the Email Archiving Hosted Service Appliance.

B.3 This SLA applies only to end-user driven search activities and not those initiated by automated systems.

B.4 This SLA applies only to calendar months in which the customer has performed greater than 250 searches.

B.5 **Remedy.** If in any calendar month the Search Performance SLA is not met and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit will be calculated in accordance with the table below.

Median of all searches (minimum of 250 searches per Calendar Month)	Service Credit
> 20 seconds	10%
> 25 seconds	15%
> 30 seconds	25%

- -

Proofpoint Digital Risk Products

Service Level Agreement

1. Standard Terms Applicable to each SLA:

A. Definitions. Except as otherwise modified or defined herein, all capitalized terms in this Digital Risk Products Service Level Agreement (SLA) have the same meanings as set forth in the Proofpoint Customer Agreement or the Proofpoint Master Subscription Agreement (the "Agreement"). For purposes of this Digital Risk Products SLA the following definitions will apply.

A.1 "Digital Risk Product" means Domain Discover, Proofpoint Patrol, Proofpoint Capture, Social Discover and Social Patrol that have been assigned specific service levels within this SLA.

A.2 "**Emergency Maintenance**" means any time outside of Scheduled Maintenance Window that Proofpoint is required to apply urgent patches or fixes or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the Digital Risk Product to be unavailable during the Emergency Maintenance.

A.3 "Scheduled Maintenance Window" means the window during which monthly scheduled maintenance of the Digital Risk Product may be performed. The Scheduled Maintenance Window can occur up to three times monthly between the hours of 12:00 a.m. to 3:00 a.m. Pacific time.

A.4 "Service Credit" is defined in Section B.

A.4 "**System Availability**" means the percentage of total time during which a Digital Risk Product is available to Customer, excluding Scheduled Maintenance Window and Emergency Maintenance.

B. Service Credits

B.1 "Service Credit" means the percentage of the monthly Subscription Fees paid or payable for the Digital Risk Product that is awarded to Customer for a validated claim associated with that portion of the Digital Risk Product related to breach of the applicable SLA during that month.

B.2 In any given month Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming Digital Risk Product.

B.3 Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Digital Risk Product subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied against amounts due for an Extension Term.

C. SLA Claims

C.1 Customer must notify Proofpoint Customer Support within five (5) business days from date of incident it first believes entitles it to receive a remedy under the SLA set forth below. Failure to comply with this reporting requirement may forfeit Customer's right to receive a remedy in connection with an SLA.

C.2 For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. Proofpoint shall make information used to validate a SLA claim available for auditing by Customer at Customer's request.

C.3 In the event that more than one aspect of the Digital Risk Product is affected by the same root cause, the single SLA applicable to such Digital Risk Product of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

C.4 Except for gross negligence or willful misconduct, the remedies set forth herein represents Customer's sole and exclusive remedy for Proofpoint's breach of the SLAs defined in this SLA.

D. Exclusions

Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of the Digital Risk Product outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Proofpoint's data center and not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; (iv) a Force Majeure Event; Customer's unauthorized action or inaction from Customer's employees, agents, contractors, or vendors or anyone gaining access to Proofpoint's network by means of Customer's passwords or equipment. These SLAs do not apply to any end of life product or software version.

2. DIGITAL RISK PRODUCT AVAILABILITY SLA

A.1 Proofpoint warrants at least 99.999% System Availability of service modules for the applicable Digital Risk Product, excluding Scheduled Maintenance Window and Emergency Maintenance.

A.2 Service Availability Calculation: If the Digital Risk Product System Availability is less than 99.999%, and if Customer has fulfilled all its obligations under the Agreement and this Service Level Agreement, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet the System Availability has occurred. 2 Proofpoint Digital Risk Proofpoint cannot accurately estimate the unlikely, but possible, time required for Emergency Maintenance, due to variables beyond its control including but not limited to: SMN API functionality and stability, and Internet connectivity and network disruption outside of the Service Providers control.

A.3 Remedy. If the email System Availability is less than 99.999%, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet the email System Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

% of Email System Availability per Calendar Month	Service Credit
< 99.999%	10%
< 99. 0%	25%
< 98.0%	100%

Information and Cloud Security Platform
Service Level Agreement

1. Standard Terms Applicable to the SLA:

A. Definitions.

Except as otherwise modified or defined herein, all capitalized terms in this SLA have the same meanings as set forth in the Agreement. For purposes of this SLA, the following definitions will apply.

A.1 "**Emergency Maintenance**" means any time outside of the Scheduled Maintenance Window where Proofpoint is required to apply urgent patches or fixes or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the Platform to be unavailable during the Emergency Maintenance.

A.2 "**Platform**" means the Proofpoint Information and Cloud Security Platform console that hosts Proofpoint Service Products.

A.3 "**Service Credit**" is defined in Section B.

A.4 "**Service Product**" means Insider Threat Management (ITM), Endpoint DLP, Cloud Security Access Broker (CASB), Secure Access, Web Security, Proofpoint Intelligent Classification and Protection (PICP) or Browser and Email Isolation.

A.5 "**Scheduled Maintenance Window**" means the window during which weekly scheduled maintenance of the Platform may be performed. The Scheduled Maintenance Window is on Saturdays between the hours of 02:00am and 08:00am Coordinated Universal Time (UTC).

A.6 "**System Availability**" is defined in Section E.

B. Service Credits.

B.1 "**Service Credit**" means the percentage of the monthly Subscription Fees paid or payable for the Service Product that is awarded to Customer for a validated claim associated with that portion of the Service Product related to the breach of the applicable SLA during that month.

B.2 In any given month, Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming Service Product.

B.3 Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Service Product subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied against amounts due for an Extension Term.

C. SLA Claims

C.1 Customer must notify Proofpoint Customer Support via support ticket within five (5) business days from the occurrence of the SLA incident. Customer's claim ticket must identify which specific SLA applies and the details of the relevant incident. Distributors and channel partners may NOT open SLA tickets on behalf of Customer. Failure to comply with these reporting requirements may forfeit Customer's right to receive a remedy in connection with the SLA.

C.2 For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of the SLA to said incident. Proofpoint shall make information used to validate an SLA claim available for auditing by Customer at Customer's request.

C.3 In the event that more than one aspect of the Platform is affected by the same root cause, the single SLA applicable to such Service Product of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

C.4 In the event the Service Product for which a Service Credit applies was licensed by Customer as part of a bundle of Proofpoint products, the Service Credit will be calculated solely on the portion of license fees attributed by Proofpoint to the specific Service Product and not the entire product bundle.

C.5 Except for gross negligence or willful misconduct, the remedies set forth herein represents Customer's sole and exclusive remedy for Proofpoint's breach of the SLAs defined in this SLA.

D. Exclusions

D.1 Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of a Service Product outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware, public cloud or network infrastructure not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; or (iv) a Force Majeure Event. These SLAs do not apply to any end-of-life product or software version.

E. The following SLA applies to Proofpoint Platform System Availability

E.1 Proofpoint warrants at least 99% Platform System Availability for Customer to access the Platform during each calendar month. System Availability means the total time during which the Platform is available to Customer, excluding the Scheduled Maintenance Window and Emergency Maintenance ("System Availability").
E.2 Remedy: If Platform System Availability is less than 99% and if Customer has fulfilled all obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this Platform System Availability has occurred. The Service Credit will be calculated in accordance with the table below.

% of Platform System Availability per Calendar Month	**Service Credit**
<99%	10%
<98%	25%
<95%	50%

Secure Email Relay
Service Level Agreement

1. Standard Terms Applicable to the SLA:
A. Definitions.

Except as otherwise modified or defined herein, all capitalized terms in this SLA have the same meanings as set forth in the Agreement. For purposes of this SLA, the following definitions will apply.
A.1 "**Emergency Maintenance**" means any time outside of the Scheduled Maintenance Window where Proofpoint is required to apply urgent patches or fixes or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the SER service to be unavailable during the Emergency Maintenance.
A.2 "**Scheduled Maintenance Window**" means the window during which weekly scheduled maintenance of the Secure Email Relay (SER) service may be performed. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.
A.3. "Service Credit" is defined in Section B.
A.4 "**System Availability**" is defined in Section E.
B. Service Credits.
B.1 "**Service Credit**" means the percentage of the monthly Subscription Fees paid or payable for the SER service product that is awarded to Customer for a validated claim associated with that portion of the SER service related to breach of the applicable SLA during that month.
B.2 In any given month, Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming SER service product.
B.3 Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next SER service product subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied against amounts due for an Extension Term.
C. SLA Claims
C.1 Customer must notify Proofpoint Customer Support via support ticket within five (5) business days from the occurrence of the SLA incident. Customer's claim ticket must identify which specific SLA applies and the details of the relevant incident. Distributors and channel partners may NOT open SLA tickets on behalf of Customer. Failure to comply with these reporting requirements may forfeit Customer's right to receive a remedy in connection with an SLA.
C.2 For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. Proofpoint shall make information used to validate an SLA claim available for auditing by Customer at Customer's request.
C.3 In the event that more than one aspect of a SER service product is affected by the same root cause, the single SLA applicable to such SER service product of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.
C.4 The remedies set forth herein represent Customer's sole and exclusive remedy for Proofpoint's breach of the SLAs defined in the SLA.
D. Exclusions
D.1 Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of the SER outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Proofpoint's data center and not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; or (iv) a Force Majeure Event.
E. The following SLA applies to Proofpoint Secure Email Relay System Availability
E.1 Proofpoint warrants at least 99.9% Secure Email Relay (SER) System Availability to securely route Customer's outbound email (excluding bulk mail, newsletters and spam) and to access the SER Web console during each calendar month. System Availability means the total time during which SER is available to Customer, excluding the Scheduled Maintenance Window and Emergency Maintenance.

E.2 Remedy: If SER System Availability is less than 99.9% and if Customer has fulfilled all obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet this SER System Availability has occurred. The Service Credit will be calculated in accordance with the table below.

% of Secure Email Relay System Availability per Calendar Month	**Service Credit**
<99.9%	25%
<98%	50%
<95%	100%

Cloud Security Inline Components Service Level Agreement

1. Standard Terms Applicable to the SLA

A. Definitions.

Except as otherwise modified or defined herein, all capitalized terms in this SLA have the same meanings as set forth in the Agreement. For purposes of this SLA, the following definitions will apply.

A.1 "**Availability**" is defined in Section B.

A.2 "**Emergency Maintenance**" means any time outside of the Scheduled Maintenance Window in which Proofpoint is required to apply urgent patches or fixes or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the Service to be unavailable during the Emergency Maintenance.

A.3 "**Inline**" means the services deployed to provide real time control, visibility, and protection.

A.4 "**Management Access**" means access to the cloud administrator console.

A.5 "**Scheduled Maintenance Window**" means the window during which weekly scheduled maintenance of the Services may be performed.

A.6 "**Service**" means Proofpoint Web Security and CASB Proxy that have been assigned specific service levels within this SLA.

A.7 "**Service Credit**" is the number of days as set out in the Web Security & CASB Proxy Service Level Credits chart in section C.2, up to a cumulative total of 31 days in any twelve-month term, as a result of a breach of this SLA.

B. Service Availability

Service	**Covered Functionality**	**Availability**
Web Security & CASB Proxy	**Inline Availability**	
	Management Access Availability	99.9%

B.1. Availability. The availability of a Service is the percentage of time a Service's specified functionality is generally operating calculated per calendar month and measured using industry standard monitoring tools and software, excluding Scheduled Maintenance Window and Emergency Maintenance ("**Availability**"). Services achieving Availability, as calculated and described in this section meet the prescribed service level in the table below:

C. Service Credits

C.1 In any given month, Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming Service.

C.2 Customer's sole remedy for breach of this SLA is the receipt of Service Credits. The number of days awarded as a Service Credit is as follows:

Web Security & CASB Proxy Service Level Credits		
Inline Availability	**Management Access Availability**	**Service Credit**
> = 99.999%	> = 99.9%	None
99.99% - < 99.999%	99.0% - < 99.9%	3 days
99.00% - < 99.99%	97% - < 99.0%	8 days
98.0% - < 99.00%	95% - < 97%	15 days

< 98%	< 95%	31 days

C.3 Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Service subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied against amounts due for an Extension Term.

D. Claims Process

D.1 Customer must notify Proofpoint Customer Support via support ticket within five (5) business days from the occurrence of the SLA incident. Customer's claim ticket must identify which specific SLA applies and the details of the relevant incident. Distributors and channel partners may not open SLA tickets on behalf of Customer. Failure to comply with these reporting requirements may forfeit Customer's right to receive a remedy in connection with an SLA.

D.2 For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. Proofpoint shall make information used to validate an SLA claim available for auditing by Customer at Customer's request.

D.3 In the event that more than one aspect of the Service is affected by the same root cause, the single SLA applicable to such Service of Customer's choosing may be claimed, and no other claim will be validated or otherwise allowed for that event.

D.4 In the event a Service for which a Service Credit applies was licensed by Customer as part of a bundle of Proofpoint products, the Service Credit will be calculated solely on the portion of license fees attributed by Proofpoint to the specific Service and not the entire product bundle.

D.5 Except for gross negligence or willful misconduct, the remedies set forth herein represents Customer's sole and exclusive remedy for Proofpoint's breach of the SLA.

E. Exclusions

E.1 Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of the Service outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Proofpoint's data center and not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; (iv) unavailability of one or more specific features, functions, or equipment hosting locations within the Service, while other key features remain available; (v) Customer requests for additional configuration or system changes that require downtime to complete; or (vi) a Force Majeure Event. These SLAs do not apply to any end-of-life product or software version.

E.2 Customer is responsible for failures of the equipment or software used to access the Service.

Proofpoint PX
Service Level Agreement

1. Standard Terms Applicable to each SLA:

A. Definitions. Except as otherwise modified or defined herein, all capitalized terms in this Proofpoint PX ("Hosted Services") Services Service Level Agreement have the same meanings as set forth in the General Terms and Conditions and the applicable Product Exhibit (collectively, "Agreement"). For purposes of this Hosted Services Service Level Agreement the following definitions will apply.

A.1 "Scheduled Maintenance Window" means the window during which weekly scheduled maintenance of the Hosted Service may be performed. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.

A.2 "Emergency Maintenance" means any time outside of Scheduled Maintenance Window that Proofpoint is required to apply urgent patches or fixes, or undertake other urgent maintenance activities. If Emergency Maintenance is required, Proofpoint will contact Customer and provide the expected start time and the planned duration of the Emergency Maintenance and if Proofpoint expects the Hosted Service to be unavailable during the Emergency Maintenance.

B. Service Credits

B.1 "Service Credit" means the percentage of the monthly Subscription Fees paid or payable for the Hosted Service product that is awarded to Customer for a validated claim associated with that portion of the Hosted Service related to breach of the applicable SLA during that month.

B.2 In any given month Customer shall in no event be entitled to receive a credit that exceeds 100% of its monthly Subscription Fee for the nonconforming Hosted Service product.

B.3 Any Service Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Hosted Service product subscription period for which the Service Credit applies. Service Credits earned by Customer hereunder will be applied

against amounts due for an Extension Term. If Service Credits cannot be applied to future Subscription Fees because the Agreement has terminated due to Proofpoint's breach of the Agreement, Proofpoint will promptly pay Customer the amount of the Services Credit.

C. SLA Claims

C.1 Customer must notify Proofpoint Customer Support via support ticket within five (5) business days from the occurrence of the SLA incident. Customer's claim ticket must identify which specific SLA applies and the details of the relevant incident. Distributors and channel partners may NOT open SLA tickets on behalf of a Customer. If requested by Proofpoint, Customer will provide Proofpoint a live copy of the applicable email with the original Proofpoint headers (complete and untampered with) for analysis. Failure to comply with these reporting requirements may forfeit Customer's right to receive a remedy in connection with an SLA.

C.2 For all claims subject to validation by Proofpoint, Proofpoint will use log files, database records, audit logs, and any other information available to validate claims and make a good faith judgment on the applicability of SLAs to said incident. Proofpoint shall make information used to validate an SLA claim available for auditing by Customer at Customer's request.

C.3 In the event that more than one aspect of a Hosted Service product is affected by the same root cause, the single SLA applicable to such Hosted Service product of Customer's choosing may be claimed and no other claim will be validated or otherwise allowed for that event.

C.4 Except for gross negligence or willful misconduct, the remedies set forth herein represents Customer's sole and exclusive remedy for Proofpoint's breach of the SLAs defined in this SLA.

D. Exclusions

D.1 Customer shall not have any remedies under any SLA to the extent any SLA claim is due to: (i) use of the Hosted Service product outside the scope described in the Agreement; (ii) Customer Equipment and/or third party software, hardware or network infrastructure outside of Proofpoint's data center and not under the direct control of Proofpoint; (iii) failure of Customer to meet the configuration requirements for Customer Equipment set forth in the Documentation; or (iv) a Force Majeure Event. These SLAs do not apply to any end-of-life product or software version.

2. SECURITY SERVICES HOSTED SERVICE SLAs. The following SLAs apply to the Security Services Hosted Service.

A. Filtering System Availability SLA.

A.1 Proofpoint warrants at least 99.999% System Availability, which is defined as % of total time during which email service connectivity on port 25 is available during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance. For purposes of calculating System Availability, only downtime occurrences exceeding 30 seconds will apply.

A.2 Customer Responsibilities. Customer must: (a) configure MS Office 365 or other applicable email service provider per Proofpoint documentation; (b) identify the number of impacted users as a subset against the total number of licensed users; (c) if inbound email is impacted provide the timeframes of the Service unavailability; (d) if outbound email is impacted provide copies of impacted email with the original Proofpoint headers complete and unaltered; and (e) provide ping and trace routes.

A.3 Remedy. If the email System Availability is less than 99.999%, and if Customer has fulfilled all of its obligations under the Agreement and this SLA, Proofpoint will provide Customer with a Service Credit for the month in which the failure to meet the email System Availability SLA has occurred. The Service Credit will be calculated in accordance with the table below.

Proofpoint PX SLA 2 October 2022 **% of Email System Availability per Calendar Month**	**Service Credit**
< 99.999%	25%
< 99. 0%	50%
< 98.0%	100%

Exhibit 3 Product Specific Terms

Core Email Protection API (formerly Adaptive Email Security (AES). Cloud-based email protection solution that employs a fully integrated layer of behavioral AI to help detect and prevent inbound email compromise and lateral phishing while providing end-users with in-moment warning banners to help them decide whether an email is safe.

Application Programming Interfaces (APIs). Access to and use of any and all Proofpoint APIs is governed by the terms of the Agreement and the API Terms of Use at https://www.proofpoint.com/us/legal/api-terms-of-use.

CASB Proxy. CASB Proxy identifies and classifies regulated or sensitive data, and monitors such data as it is uploaded, downloaded or shared in the Cloud.

Closed-Loop Email Analysis and Response (CLEAR). CLEAR integrates the functionalities of PhishAlarm and TRAP to streamline Customer's end user reporting and security response to phishing attacks.

Account Takeover Protection (ATO) / Cloud Account Security Broker / CASB Protection for IaaS (add-on) / CASB OCR (add-on). Proofpoint Account Takeover Protection (ATO) helps Customer detect suspicious activities around Customer's cloud accounts and identify compromised cloud accounts. Proofpoint Cloud Account Security Broker uses policies to prevent the loss of Customer's sensitive or confidential data contained in Customer's cloud accounts. CASB IaaS Protection helps customer identify its IaaS resources, protect sensitive data within IaaS storage, and monitor and stop unauthorized logins to Customer's Cloud accounts. CASB Protection for IaaS is subject to the DLP traffic limitation described in the quote or Order Form. CASB OCR technology for DLP extracts and analyzes text content in images to identify sensitive information. CASB OCR is subject to the image limitation described in the quote or Order Form.

Cloud Threat Response. Cloud Threat Response is a cloud-based email security solution used to respond to threats through automated and manual processes. The solution ingests threat information from multiple alert sources and integrates with the customer's mail server (Exchange, Office 365, G Suite) to retrieve and move messages.

Cloudmark Products. Cloudmark Products include Cloudmark Authority, Cloudmark Safe Messaging Cloud (SMC), and Cloudmark Spam Reporting Service (SRS). Cloudmark Products leverage intelligent threat analysis to provide email, SMS and mobile messaging security against spam and malware. Notwithstanding anything to the contrary in the Agreement, the parties hereby agree that Work Product resulting from Professional Services for Cloudmark Products includes Customer configurations. Proofpoint grants to Customer a license to such Work Product (including Customer configurations) pursuant to the Agreement. Additionally, Customer acknowledges that use of the "Cloudmark Network Feedback System" involves sending unencrypted Customer e-mail and spam samples into this system. This process is optional for the Customer and only occurs for an email message when a User chooses to click on the "This is Spam" button or the "This is NOT spam" button for a given email message. Proofpoint analyses theses spam reports and unblock reports in order to increase the accuracy of the Proofpoint Product. Customer's license to Use Cloudmark Products includes the right to use the Cloudmark Products for the benefit of Customer's end user customers, pursuant to a written license agreement between Customer and each end user customer that is at least as protective of Proofpoint's rights as the terms of the Agreement and this Exhibit.

Continuity. Continuity provides temporary storage of Customer inbound and outbound email within the on-demand, Web-based email. Continuity is limited to the number of calendar days and the maximum per User data volume set forth in the Order Form or Proofpoint quote. Customer acknowledges that Continuity is only to serve as a secondary, emergency failover option in the event of failure of Customer's email service, and not to serve as a primary email archive solution or a primary failover solution. Customer is required to have a current subscription for Proofpoint email protection to use Continuity.

Continuity Plus. Continuity Plus provides temporary storage of Customer inbound and outbound email within the on-demand, Web-based email. Continuity Plus is limited to the number of calendar days and the maximum per User data volume set forth in the Order Form or Proofpoint quote. Continuity Plus is licensed on a User basis Customer must: (i) enable the email journaling feature within Customer's Microsoft Exchange Server, or Microsoft Office 365 service; and (ii) ensure that the Customer's network has proper policies to allow journaling emails to be transmitted to the Proofpoint hostnames and IP addresses for Continuity Plus. This feature for emergency storage of outbound and intra-domain email is only supported for select versions of Microsoft Exchange Server and Microsoft Office 365.

Data Discover. Data Discover scans emails, files on network shared drives, and cloud storage services to find and track protect sensitive information (such as PII, PHI and GDPR Personal Data) so Customers can identify data risks and determine appropriate remediation.

Domain Discover. Domain Discover identifies suspicious domains that fraudulently use, impersonate or look like Customer's legitimate domains and trademarks. Customer is responsible for acquiring all necessary data subject consents. Customer is responsible for maintaining the user accounts and the security of its user names and passwords at the user level and for promptly changing or deleting any user name or password that Customer believes may have been compromised. Proofpoint reserves the right to institute password requirements (such as the length of password or the required use of numbers, symbols etc.) and to refuse registration of, or cancel passwords it deems inappropriate. The Proofpoint Products may allow Customer to interface with a variety of third party software or services (e.g., Facebook, Twitter, LinkedIn). No endorsement of any such service should be inferred as a result of any integration with the Proofpoint Products and Proofpoint is not responsible for the data, operation or functionality of such

third-party services. While Proofpoint may, in its sole discretion, customize the Proofpoint Products to interoperate with various third-party services: (a) Customer is responsible for complying with the terms and policies of each such third-party service including, without limitation, any payment obligations related thereto; and (b) Proofpoint cannot guarantee that such third-party services will continue to interoperate with the Service.

Email Brand Defense (EBD). Using DMARC and threat intelligence, EBD identifies and blocks malicious emails, spoofing trusted brands and domains, before they hit consumer inboxes.

Email Data Loss Prevention (DLP). Email DLP utilizes policies to prevent the loss of Customer's sensitive or confidential data through email.

Email Encryption. Proofpoint Email Encryption provides a fully integrated message encryption and decryption solution.

Email Exfiltration Protection. Email Exfiltration Protection is a cloud-based email protection service that prevents exfiltration to unauthorized accounts, and potential loss of proprietary data and intellectual property without predefined rules or deny lists.

Email Fraud Defense (EFD). EFD blocks spear phishing emails spoofing trusted domains and evaluates the authenticity of senders to block emails from unauthenticated sources.

Email Protection. Email Protection includes functions such as spam detection functions to identify and classify spam messages; virus protection functions to detect and filter messages containing known viruses; zero-hour anti-virus functions to detect and filter messages containing suspicious content; a quarantine folder to analysis and disposition of suspicious content; and Proofpoint Dynamic Reputation functions to terminates connection from IP addresses that have displayed poor reputation. Email Protection is for use with normal external business messaging traffic only, and Customer shall not use Email Protection for the machine generated message delivery of bulk or unsolicited emails or emails sent from an account not assigned to an individual. Customer is responsible for maintaining the outbound email filtering Email Protection configuration settings to block emails identified by Proofpoint as either containing a virus or having a spam score of ninety-five (95) or higher. If Proofpoint has reason to believe that Customer has modified the outbound email configuration setting, Proofpoint reserves the right to monitor and reset such settings. If Customer is licensed for the SaaS deployment of Email Protection Customer is prohibited from deactivating the Dynamic Reputation feature. Each User must be assigned a separate account on Customer's email server for sending or receiving messages or data within Customer's email system or network. If requested in writing, Proofpoint will set up the Customer's instance of the Email Protection product within Proofpoint's U.S. gateways or data centers. So long as Customer configures its MX records to point to URLs provided to Customer by Proofpoint for the instance in the United States, Customer's email will be filtered in US based data centers.

Email Threat Defense. Email Threat Defense is a cloud-based email defense service which uses machine learning to detect and prevent inbound email attacks, while providing end-users with in-moment contextual warning banners to help them decide whether an email is safe.

Emerging Threats Intelligence. ET Query, ET Pro Ruleset and ET Reputation are data feeds and may include network intrusion detection signatures, global intelligence portal, intelligence APIs, and reputation lists to enable Customer to detect and investigate network-based threats in or against its environment.

Endpoint Data Loss Prevention (Endpoint DLP). Endpoint Data Loss Prevention is hosted on the Information and Cloud Security Platform and deploys software (an Agent) onto Customer owned or controlled desktops and servers on supported platforms. These Agents capture metadata recorded from the activities of licensed Users and store this data in Proofpoint's Endpoint DLP service. A licensed User of Endpoint DLP is a unique individual with a unique access credential being monitored by Customer, regardless of whether the Agents are deployed on physical or virtual systems. If an individual has more than one access credential, then a separate User license for each of that individual's unique access credentials must be purchased. A licensed User of Endpoint DLP may also be a unique Server (physical or virtual) with a unique access credential being monitored by the Customer. Endpoint DLP Metadata Feed allows Customer to export its captured User metadata. Endpoint DLP Metadata Feed is subject to a maximum monthly export amount as described in the Proofpoint quote or Order Form. Excessive ingestion of activities may lead to local caching on an Agent or throttling of transmission to the cloud.

Essentials. Please see the attached EULA found at: https://www.proofpoint.com/sites/default/files/legal-documents/pfpt-en-essentials-eula.pdf.

Insider Threat Management (ITM). ITM SaaS is hosted on the Information and Cloud Security Platform and deploys software (an Agent) onto Customer managed desktops, laptops, virtual machines, and servers. These Agents capture metadata (Metadata Capture) and visual screen content (Visual Capture) recorded from the activities of monitored Users and store this data in Proofpoint's Information and Cloud Security Platform. ITM SaaS Metadata Feed allows Customer to export its captured User metadata. A licensed User of ITM SaaS is a unique individual with a unique access credential being monitored by Customer, regardless of whether the Agents are deployed on physical or virtual systems. If an individual has more than one access credential, then a separate User license for each of that individual's unique access credentials must be purchased. A licensed User of ITM SaaS may also be a unique Server (physical or virtual) with a unique access credential being monitored by the Customer. ITM SaaS Metadata Capture, and ITM SaaS Metadata Capture with Visual Capture, are subject to the activity ingestion rate(s) and retention time tiers described in the Proofpoint quote or Order Form. Additionally, both the ITM SaaS Metadata Capture with Visual Capture and ITM Additional Visual Capture are further subject to the aggregate data storage limit(s) described in the Proofpoint quote or Order Form. ITM SaaS Metadata Feed is subject to a maximum monthly export amount as described in the Proofpoint quote or Order Form. Excessive

ingestion of User activities may lead to local caching on an Agent or throttling of transmission to the cloud. Proofpoint reserves the right to require that the Customer pay additional fees when any ingestion, storage, and/or export limit is exceeded. ITM On-Prem is deployed on customer-provided infrastructure (bare-metal, VMs or customer-managed cloud) and Proofpoint does not have access to the customer's deployment. Proofpoint licenses the On-Prem version based on the number of endpoints the Agent is installed on.

Intelligent Classification and Protection. Proofpoint Intelligent Classification and Protection AI engine automatically locates and identifies sensitive and business-critical data to enhance existing data protection solutions such as labeling, encryption, access control, data loss prevention, CASB and suggests protection rules and/or policies to the Customer.

Internal Mail Defense (IMD). IMD leverages Email Protection and TAP features to protect Customer's internal email communications against spam and malicious content.

Misdirected Email Protection. Misdirected Email Protection is a cloud-based email protection service that prevents accidental data loss from misdirected emails and misattached files, preventing sensitive information being inadvertently sent to an unintended recipient.

Nexus People Risk Explorer. Proofpoint Nexus People Risk Explorer leverages people centric security data from Proofpoint's Targeted Attack Protection, Security Awareness Training, Cloud Account Defense and Cloud Account Security Broker to provide insights into the types, severity and frequency of threats targeted at Customer and its employees.

PhishAlarm & PhishAlarm Analyzer. PhishAlarm allows end users to report phishing emails and other suspicious messages. PhishAlarm Analyzer delivers highly responsive identification of phishing attacks in real time. Emails reported via PhishAlarm & PhishAlarm Analyzer are accessed and categorized and they are immediately available to Customer's response teams.

Proofpoint Archive. Proofpoint Archive is a cloud-based archiving solution designed for legal discovery, regulatory compliance and data access for Customer's end users, and it provides a central, searchable repository that supports a wide range of content types. Upon termination or expiration of Customer's license to use the Proofpoint Product, for a period of thirty (30) days after termination or expiration ("Wind Down Period") subject to payment of a pro-rata fee Customer may continue to access and retrieve its data that has been stored in the Archive product prior to termination. During the Wind Down Period, Customer may not use the Proofpoint Product to archive new email messages. For an additional fee, Proofpoint will export customer's data for delivery to Customer on standard storage media. If Proofpoint has not received a written request from Customer to export customer's data prior to the end of the Wind Down Period, Proofpoint will initiate the removal of customer's data in such a manner that it cannot be restored in human readable form from any and all storage mediums (including backups), which will be completed within thirty (30) days.

Proofpoint Automate. Proofpoint Automate uses machine learning to evaluate supported archived messages (such as email, social media, collaboration platforms, and mobile messages) flagged for Customer's review by Proofpoint Supervision. This helps Customer improve its regulatory supervision decision making and automate key parts of Customer's supervision workflow. Customer may configure its own data models in the supervision UI. As between Proofpoint and Customer, Proofpoint shall have no liability whatsoever with respect to such data models. If Proofpoint has reason to believe that a data model is malfunctioning, Proofpoint reserves the right to disable the data model.

Proofpoint Capture. Proofpoint Capture captures content from supported messaging and Cloud storage platforms and delivers it compliance services such as e-discovery, archive and supervision.

Proofpoint Certification Exam. Proofpoint Certification Exam allows individuals to take exams covering different Proofpoint products and technologies. Exam takers will receive a Proofpoint subject matter certification for each individual exam they pass.

Proofpoint Certification Exam Training. Proofpoint Certification Exam Training provides access to live instructor-led and online self-paced training courses to prepare exam takers for the Proofpoint Certification Exam.

Proofpoint Collab Protection. Provides browser level threat protection to help protect users from URL based attacks. Includes protection for URLs delivered through channels such as collaborative apps (Slack, Teams), messaging apps (Messenger, WhatsApp), and social media (LinkedIn, Facebook). Reporting for Collab Protection is available in the TAP Dashboard.

Proofpoint Data Security Posture Management (DSPM). Automatically discovers, classifies, and enables prioritized remediation of security and compliance risks across supported data types, including AI/ML pipelines, within cloud and on-premises environments.

Proofpoint Discover. Proofpoint Discover is an add-on capability to Proofpoint's Archive service with case management features, advanced visualizations and Technology Assisted Review for classifying electronically stored information (ESI) for legal discovery.

Proofpoint Isolation. Proofpoint Isolation products establish an isolated remote web browser or web email environment to protect the Customer from potential threats when Users connect to the Internet or web-based email accounts on Customer owned or controller devices. Customer will not allow Users to transmit through (or post on) Isolation any infringing, defamatory, threatening or offensive material.

Proofpoint Patrol. Proofpoint Patrol allows Customers to monitor, remediate and generate compliance reports about their end users' activities on Customer controlled social media accounts. Proofpoint Patrol for Text is the limited version of Proofpoint Patrol

exclusively for third-party text messaging applications. Proofpoint Patrol uses YouTube API Services, please see Google's Privacy Policy at http://www.google.com/policies/privacy.

Proofpoint PX. Proofpoint PX is a cloud-based solution that leverages Email Protection, TAP, and Threat Response Cloud to provide functions to detect and filter messages with threats such as Business Email Compromise (BEC), phishing, and malware; message quarantines for analysis and disposition of suspicious content; and functions to quarantine delivered messages with threats. Proofpoint PX is for use with normal external business messaging traffic flowing through a Microsoft O365 application instance only. Customer shall not use Proofpoint PX for the machine generated message delivery of bulk or unsolicited emails or emails sent from an account not assigned to an individual.

Proofpoint SaaS & Identity Posture Management. Automatically discovers, prioritizes, and guides the remediation of security risks with SaaS applications and identity providers. It also provides visibility into unsanctioned SaaS applications.

Proofpoint Shadow. Proofpoint Shadow detects attackers who have already gained access to Customer's network and prevents further access against Customer's critical assets. Shadow deploys believable, automatically customized, assets that mimic the data, credentials, and connections that attackers seek. Shadow triggers incidents and collects real-time forensics from compromised Customer endpoints to assist in triage and risk response.

Proofpoint Spotlight. Proofpoint Spotlight is an identity threat detection and response (ITDR) solution that automatically discovers, prioritizes, and remediates identity vulnerabilities through Customer's corporate network. Spotlight detects directory structure misconfigurations in Active Directory and Azure AD, searches for accounts unmanaged by PAM, and detects and eliminates exposed credentials on Customer's endpoint devices.

Proofpoint Supervision. Proofpoint Supervision is a cloud-based solution that helps Customer identify, review, address and maintain audit trails from the Customer's regulatory data archive, including all incoming, outgoing and internal correspondence captured by Customer's archive.

Proofpoint Takedown. Proofpoint Takedown helps Customers safeguard against URL and domain-based attacks. Customers submit a takedown request to initiate the process of mitigating malicious domain and URL activity targeting Customer.

Proofpoint Track. Proofpoint Track acts as a central hub to filter and route message content to Customer's archive, supervision and analytic systems.

Secure Access. Proofpoint Secure Access is a people-centric, zero- trust alternative to VPN. It secures remote access to any enterprise application, regardless of location. Secure Access provides Users microsegmented secure access to hundreds of cloud instances. Customers can automate cloud-to-cloud connectivity and quickly deploy access from user devices to apps in both on-premises data centers and public clouds.

Secure Email Relay. Secure Email Relay (SER) is a hosted, multi-tenant solution that puts Customer in control of applications that send email using Customer's owned or controlled domains. It adds a layer of security to each application and distributes the email to the Internet in a DMARC-compliant fashion after Proofpoint AS/AV checks are performed. SER may only be used for delivery of emails that comply with applicable bulk or unsolicited message laws. The number of messages processed through SER is limited to the annual amount identified in the Proofpoint quote or Order Form and Proofpoint reserves the right to require that the Customer pay additional fees when such limit is exceeded. Additionally, any processing of messages in excess may lead to throttling of message transmission. Customer must protect SER credentials and only use SER for the intended application.

Social Discover. Social Discover scans the Internet to identify accounts using Customer's brands on social media networks, including unauthorized accounts.

Social Patrol. Social Patrol automatically scans Customer's social media account posts and comments for high-risk content such as malware, phishing links, hate speech, pornography and piracy.

Supplier Threat Protection. Designed to identify customer's suspected supplier and/or known third-party compromised email accounts. The customer is made aware of the potential suspicious account through the TAP Dashboard, allowing a customer to proactively investigate and/or take action to protect their environment from a supplier and/or known third-party compromised account.

Targeted Attack Protection (TAP). TAP identifies and protects against malicious URLs and malicious attachments in emails using a dynamic malware analysis engine.

Threat Response. Threat Response is an incident management platform that leverages event source alerts, automation, reporting, threat intelligence and IOC agents to enable Customer to manage cybersecurity threats. Threat Response interoperates with certain supported: (i) third-party data sources ("*Event Source*"); (ii) quality and data enrichment sources ("Enrichment Sources"), and (iii) third-party security enforcement platforms (e.g. firewalls, and web proxy servers) ("*Enforcement Device*"). As between Proofpoint and Customer, Proofpoint shall have no liability whatsoever with respect to the accuracy, availability, or quality of Event Sources, Enrichment Sources or Enforcement Devices. Customer may configure additional Event Sources and Enforcement Devices as needed by Customer in connection to Customer's use of Threat Response.

Threat Response Auto Pull (TRAP). TRAP is an incident management platform that includes automation to analyze and remove unwanted emails. Threat Response Auto Pull may only be integrated with Event Sources, (i) Enrichment Sources, or (ii) Microsoft Exchange Server, Microsoft Office 365, Google Gmail or IBM Domino as an Enforcement Device; and can only be used with the following data Event Sources: Proofpoint TAP, Abuse Mailbox Monitor, FireEye EX, Proofpoint Smart Search results, Splunk (events for email quarantine only) and JSON (events for email quarantine only). Upon written notice (via email) to Customer's Named Support Contact from Proofpoint, Customer will send a copy of its specific TRAP system configuration to Proofpoint for review.

Web Security / Web Security OCR (add-on). Proofpoint Web Security protects Users against advanced threats when they browse the web. It supports a Customer's distributed workforce by ensuring secure internet access for all workers, whether they're inside or outside of Customer's perimeter. It applies monitoring and visibility, advanced threat protection and data-loss prevention (DLP) policies in a people-centric approach to security. Web Security does not support routing streaming media through the proxy. Web Security OCR technology automatically extracts and analyzes text content in images to identify sensitive information and is subject to the image limitation described in the quote or Order Form.

ZenGuide (formally known as Proofpoint Security Awareness aka PSAT). ZenGuide offers a comprehensive approach to cybersecurity education, leveraging diverse learning methods to enhance organizational security. The solution delivers content in multiple languages, ensuring global accessibility while promoting diversity, equity, and inclusion. ZenGuide incorporates timely threat-specific information, microlearning modules, and compliance training, alongside real-world simulations and nudging techniques to reinforce best practices. Key features include automated learning paths, personalized experiences, and adaptive assessments, all supported by robust multi-tenant administration as well as reporting and dashboard tools that enable administrators to track individual progress and overall program effectiveness."

END OF AGREEMENT