Symantec™ Email Fraud Protection

Service Description

December 2018

This Service Description describes Symantec's Email Fraud Protection ("Service"). All capitalized terms in this description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Customer's manually or digitally-signed agreement with Symantec which governs the use of the Service, or if no such signed agreement exists, the Symantec Online Services Terms and Conditions (hereinafter referred to as the "Agreement").

Table of Contents

1: Technical/Business Functionality and Capabilities

- Service Overview
- Service Level Agreement
- Supported Platforms and Technical Requirements
- Hosted Service Software Components

2: Customer Responsibilities

- Acceptable Use Policy

3: Entitlement and Subscription Information

- Charge Metrics
- Changes to Subscription

4: Assistance and Technical Support

- Customer Assistance
- Technical Support
- Maintenance to the Service and/or supporting Service Infrastructure

5: Additional Terms

6: Definitions

Exhibit-A Service Level Agreement

Symantec™ Email Fraud Protection

Service Description

December 2018

1: Technical/Business Functionality and Capabilities

Service Overview

Symantec™ Email Fraud Protection is a cloud service that automates enforcing DMARC (Domain-based Message Authentication, Reporting, and Conformance).

Service Features

- The Service is provided for the number of Users for the Subscription Term.
- Customer Administrators can access the Email Fraud Protection management console by using a secure password-protected login. The Email Fraud Protection management console provides the ability for Customer Administrators to configure and manage the Service, access reports, and view available data and statistics.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- Reporting for the Service is available through the Email Fraud Protection management console. Reporting may include activity logs and/or statistics. Using the management console, Customer Administrators may choose to generate reports, which can be configured to be sent by Email on a scheduled basis or downloaded from the management console.

Service Level Agreement

- Symantec provides the applicable service level agreement ("SLA") for the Service as specified in Exhibit-A.

Supported Platforms and Technical Requirements

- Supported platforms and technical requirements for the Service are provided at https://help.symantec.com/home/FRAUD_PRO?locale=EN_US.

2: Customer Responsibilities

Symantec can only deliver the Service if Customer provides required information or performs required actions. Otherwise, the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Customer is responsible for modifying the DNS records or other necessary settings for domains, as outlined in Email Fraud Protection documentation, in order to enable the Authentication Services for those domains. At the end of Customer subscription, Customer is responsible for restoring those records or settings to their original state.
- Customer is responsible for maintaining the confidentiality of any user IDs, passwords and other credentials associated with Customer account.
- Customer is responsible for all acts, omissions, and breaches by its Authorized Users..
- Customer is responsible for Authorized Users' use of the Authentication Services and compliance with the Subscription Terms.
- Customer is responsible for any Customer-furnished data.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Subscription Instrument or Order Confirmation within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Service Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the Email Fraud Protection management console, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control, therefore, Symantec is not

liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

Acceptable Use Policy

- Customer is responsible for complying with the Symantec Online Services Acceptable Use Policy.

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under the following Meter as specified in the Order Confirmation:

- "**User**" means an individual person and/or device authorized to use and/or benefits from the use of the Service, or that actually uses any portion of the Service.

Changes to Subscription

If Customer has received Customer's Subscription or Entitlement directly from Symantec, communication regarding permitted changes of Customer's Subscription or Entitlement must be requested at the following address (or replacement address as published by Symantec): https://go.symantec.com/customercare, unless otherwise noted in Customer's agreement with Symantec. Any notice given according to this procedure will be deemed to have been given when received. If Customer has received Customer's Subscription or Entitlement through a Symantec reseller, please contact Customer's reseller.

4: Assistance and Technical Support

Note: This section only applies if Customer is entitled to receive Customer Assistance and Support directly from Symantec ("Support"). If a Customer is entitled to receive Assistance and Support from a Symantec reseller, refer to Customer's agreement with that reseller for details regarding such Support, and the Support described here will not apply to Customer.

Customer Assistance

Symantec will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service;
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions.

Technical Support

Entry-level Support is included as part of the Service as specified below.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published terms and conditions and technical support policies published at https://www.symantec.com/docs/TECH236428.
- Once a severity level is assigned to a Customer submission for Support, Symantec will make every reasonable effort to respond per the response targets defined in the table below. Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Support commitment.

Problem Severity	Support (24x7) Response Targets*
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a	Within 30 minutes

substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	Within 2 hours
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	By same time next business day**
Severity 4: A problem has occurred where Customer's business operations have not been adversely affected.	Within the next business day; Symantec further recommends that Customer submit Customer's suggestion for new features or enhancements to Symantec's forums

The above Support Response Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.

** Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the request).*

*** A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding weekends and local public holidays. In most cases, "business hours" mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone.*

Maintenance to the Service and/or supporting Service Infrastructure

Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance.* "**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Symantec uses commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low. The scheduled time for maintenance is 9:00 p.m. to 3:00 a.m. PST/PDT, and Symantec may perform maintenance during this time with no advance notification to Customer.
- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance. As used herein, "**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.
- *Email Fraud Protection Management Console Maintenance.* Symantec will use commercially reasonable efforts to perform maintenance on the management console at times when collective Customer activity is low to minimize disruption to the availability of the Email Fraud Protection management console. Customer will not receive prior notification for these routine maintenance activities.

5: Additional Terms

- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Symantec reserves the right to modify and update the features and functionality of the Service, with the objective of providing equal or enhanced Service (as long as Symantec does not materially reduce the core functionality of the Service). Customer acknowledges and agrees that Symantec reserves the right to update this Service Description at any time during the Subscription Term to accurately reflect the Service being provided, and the updated Service Description will become effective upon posting.
- Except as otherwise specified in the Service Description, the Service may use open source and other third-party materials that are subject to a separate license.
- Customer shall comply with all applicable laws with respect to use of the Service. Configuration and use of the Service(s) is entirely in Customer's control; therefore, Symantec is not liable for Customer's use of the Service(s), nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

- In the event that continued provision of the Service to Customer would compromise the security of the Service, including but not limited to hacking attempts, denial of Service attacks, mail bombs or other malicious activities either directed at or originating from Customer's domains, Customer agrees that Symantec may temporarily suspend Service to Customer. In such an event, Symantec will promptly inform Customer and will work with Customer to resolve such issues. Symantec will reinstate the Service upon removal of the security threat.
- Should the Service be suspended for any reason whatsoever, the Service will not be available.
- Should the Service be terminated for any reason whatsoever, Customer's account will be deleted, and Customer will not have access to the Service.
- Customer is permitted to use the Service solely for Customer's own business purposes. Customer agrees not to resell, sublicense, lease, or otherwise make the Service and associated documentation available to any third party. Customer agrees not to use the Service for the purposes of building a competitive product or service or copying its features or user interface, performing Service evaluations, benchmarking or other comparative analysis intended for publication outside Customer organization without Symantec's prior written consent.

6: Definitions

"**Administrator**" means a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.

"**Authentication Services**" means the web-based services included in your subscription plan that are facilitated by the Email Fraud Protection cloud platform.

"**Authorized User**" means an individual employee or agent of the Customer who has been assigned unique credentials to access and use the Authentication Services, whether or not that individual is accessing or using the Authentication Services at any particular time.

"**Credit Request**" means the notification which Customer must submit to Symantec by Email to support.cloud@symantec.com with the subject line "Credit Request" (unless otherwise notified by Symantec).

"**Infrastructure**" means any Symantec or licensor technology and intellectual property used to provide the Services.

"**Monthly Charge**" means the monthly charge for the affected Service(s) as defined in the Agreement.

"**Online Help**" means the additional information available at https://help.symantec.com/home/FRAUD_PRO?locale=EN_US.

"**Order Confirmation**" has the meaning given in the Symantec Online Services Terms and Conditions, if applicable. If there are no such terms and conditions applicable to the Service, then "Order Confirmation" shall mean the Subscription Instrument, as defined herein.

"**Service**" means the Email Fraud Protection, purchased by Customer.

"**Service Credit**" means the amount of money that will be credited to Customer's next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

"**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes, or follows the Service.

"**Symantec Hosted Service Terms**" means the Symantec Hosted Services Terms located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

"**Symantec Online Service Terms and Conditions**" means the Online Services Terms and Conditions located at or accessed through https://www.symantec.com/about/legal/service-agreements.jsp.

"**User**" means an individual person sending and receiving email.

Exhibit-A
Service Level Agreement

General

- Customer may be entitled to a Service Credit if Symantec does not meet the defined service level. If Customer believes it is entitled to a Service Credit, Customer must submit a Credit Request within ten (10) business days of the end of the calendar month in which the suspected service level non-compliance occurred.
- A Credit Request is made by contacting Symantec Technical Support. Please access the product support landing page, https://go.symantec.com/customercare, and open a support case.
- All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement. Symantec may request additional information from Customer to validate the Credit Request.
- This Service Level Agreement will not operate: (i) during periods of Planned Maintenance or Emergency maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) during any period of suspension of service by Symantec in accordance with the terms of the Agreement; (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); (iv) where Customer has not configured the Service in accordance with the Agreement; or (v) during trial service periods.
- The remedies set out in this Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this Service Level Agreement.
- The maximum accumulative liability of Symantec under this Service Level Agreement in any calendar month shall be a credit equal to the lower of 100% of the Monthly Charge or ten thousand dollars/five thousand pounds sterling/ten thousand euro ($10,000/£5,000/€10,000) (depending on the currency in which Customer is invoiced).
- If the affected Service is purchased as part of a Services bundle, then the Service Credit will be calculated based on the affected Service and not on the entire Services bundle.

Service Availability

This service level shall not apply if the Customer has incorrectly configured the Service or due to unforeseen circumstances or causes beyond Symantec's reasonable control, including but not limited to natural disaster, war, terrorism, riot, government action, or a network or device failure external to Symantec's data centers, including at Customer's site or between Customer's site and Symantec's data center.

If Service Availability is below one hundred percent (100%) in any calendar month, Customer may submit a Credit Request and may receive a Service Credit for the following percentage credit equal to the lower of 100% of the Monthly Charge or ten thousand dollars/five thousand pounds sterling/ten thousand euro ($10,000/£5,000/€10,000) (depending on the currency in which Customer is invoiced):

Percentage Available Per Calendar Month	Percentage Credit Of Monthly Charge
below 100% and above or equal 99%	25%
below 99% and above or equal 98%	50%
below 98%	100%

If Service Availability falls below ninety-eight percent (98%) in any calendar month, as confirmed by Symantec, Customer shall be entitled to terminate the affected Service and receive a pro-rata refund of fees paid in advance for the portion of the term after such termination is effective.

24x7 Technical Support and Fault Response

Technical Support is available twenty-four (24) hours/day, seven (7) days/week to:
a) provide technical support to Customer for problems with the Service; and
b) communicate with Customer to resolve such problems.