Validation & ID Protection (VIP) Service

SaaS Listing

The definitions set out in the Agreement will apply to this SaaS Listing document.

The Broadcom software program(s) ("Broadcom Software") listed below listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the Broadcom quote, order, or other "Transaction Document" entered into by you and the Broadcom entity ("Broadcom") through which you obtained a license for the Broadcom Software or Service (hereinafter referred to as the "Agreement"). These terms shall be effective from the effective date of such Transaction Document.

This SaaS Listing describes Symantec Validation & ID Protection ("VIP" or "Service") and its software equivalent, VIP Authentication Hub, including all enabling components. All capitalized terms in this Listing have the meaning ascribed to them in the Agreement or in the Definitions section.

Table of Contents

Validation & ID Protection (VIP) Service

SaaS Listing

1: Technical/Business Functionality and Capabilities

Service Overview

VIP is a multi-factor authentication platform. The Service provides online service providers and enterprises with increased security of their applications in the form of multi-factor authentication and protection for their End Users against account takeover. The Service also enables End Users to utilize a single Authenticator across all VIP-enabled service providers and enterprises.

This SaaS Listing outlines the primary elements of the Service and describes the roles and responsibilities of all the entities necessary to provide strong authentication to End Users.

Service Features and Components

The Service leverages a shared validation infrastructure operated by Broadcom that enables Customer to deploy and accept multi-factor authentication without bearing the entire burden of managing and operating their own self-standing authentication infrastructure. By allowing End Users to leverage a single Authenticator to secure their transactions at multiple enterprises, Symantec VIP helps make it simpler for End Users to adopt stronger authentication.

Subject to Exhibit A (Service Level Agreement), the Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.

Key features and components:

- VIP Authenticators
- VIP Web Services Application Programming Interfaces (APIs) and Integrations
- VIP Manager
- My VIP
- VIP Self-Service Portal
- Audit Trails and Audit Retention

VIP Authenticators

An "**Authenticator**" is something End User possesses and controls (typically a cryptographic module) that is used to authenticate End User's identity claims in online interactions. The Service provides and supports several different types of VIP Authenticators: hardware and software based, as well as Out-Of-Band (OOB) Authenticators.

- **VIP OTP Tokens, Cards, and VIP Access software Authenticators –** These Authenticators are single-factor one-time password (OTP) Authenticators that generate OTPs, referred to as *security codes* in VIP. These are hardware Authenticators and software-based OTP generators installed on devices such as mobile phones and personal computers. These VIP Authenticators consist of a unique VIP Credential ID and an embedded secret, shared with the Service that is used as the seed for generation of OTPs and does not require activation through a second factor. The "VIP Credential ID" is an alphanumeric string that can vary in length from 12 to 16 characters, which identifies both the VIP Authenticator manufacturer as well as the VIP Authenticator itself. This VIP Credential ID can be bound to a "User ID," which can be any string that uniquely identifies an End User within Customer. The OTP is displayed on the device and manually input by End User for transmission to the Service for verification, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. These VIP Authenticators are anonymous and provide a second authentication factor as something End User has when it is associated to a local user identity of Customer.

- **Multi-Factor One Time Password (OTP) Authenticator –** These Authenticators are multi-factor one-time password Authenticators that generate OTPs. A multi-factor OTP Authenticator generates OTPs for use in authentication after activation through an additional

authentication factor. Only hardware-based Authenticators are available for this category. The second factor of authentication is achieved through some kind of integrated entry pad. The OTP is displayed on the Authenticator and manually input by End User for transmission to the Service for verification, thereby proving possession and control of the Authenticator. This VIP Authenticator is anonymous and provides a second authentication factor as something End User has when it is associated with a local user identity of Customer. The multi-factor OTP Authenticator is something Customer has, and it will be activated by something Customer knows.

- **VIP Security Key –** These are single-factor cryptographic Authenticators that operate by signing a challenge nonce presented through a direct computer interface (e.g., a USB port). The Authenticator uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second factor of authentication. These Authenticators have a unique VIP Credential ID, and authentication is accomplished by proving possession of the Authenticator via the Universal 2nd Factor (U2F) authentication protocol. The VIP Security Key is a multi-modal Authenticator and can also generate an OTP. This VIP Authenticator is anonymous and provides a second authentication factor as something End User has when it is associated with a local user identity of Customer.

- **VIP Trusted Device –** This Authenticator is a single-factor cryptographic software. This Authenticator consists of a cryptographic key stored on disk and associated with a unique VIP Credential ID. It utilizes a browser plug-in to manage cryptographic keys generated and stored in a proprietary keystore on End User's device. Authentication is accomplished by proving possession of the device. The Authenticator's output is provided by direct connection to the user endpoint, facilitated by the browser plug-in, and consists of a signed message. This is used as a second authentication factor when it is associated with a local End User identity at Customer.

- **VIP Push –** This is an Out-of-Band (OOB) authentication mechanism that allows the Service to send a push notification to a uniquely addressable VIP Access software Authenticator on a device in possession of End User (where VIP Push is available). The Service then waits for the establishment of an authenticated protected channel and verifies the Authenticator's identifying key and a digital signature over the contents of the message sent to the device. This signature along with End User's approval or denial of the push notification provides a second authentication factor as something End User has when it is associated with a local user identity of Customer.

- **VIP SMS OTP –** This is an Out-of-Band Authentication mechanism that allows the Service to send an OTP via a text message to an End User's SMS capable mobile device. The SMS text message contains a numeric OTP, securely generated by the Service, along with a message specified by Customer. The OTP is then manually input by End User for transmission to the Service for verification, thereby proving possession and control of the SMS device. This is used as a second authentication factor when it is associated to a local End User identity at Customer.

  SMS OOB Authentication is an additional service that may be purchased for an additional fee as a corollary to the VIP Authentication Service.

- **VIP Voice OTP –** This is an Out-of-Band Authentication mechanism that allows the Service to send an OTP via a voice call to an End User's voice capable device. The voice call contains a numeric OTP, securely generated by the Service, along with a message specified by Customer. The OTP is then manually input by End User for transmission to the Service for verification, thereby proving possession and control of the device. This is used as a second authentication factor when it is associated with a local End User identity at Customer.

  Voice OOB Authentication is an additional service that may be purchased for an additional fee as a corollary to the VIP Authentication Service.

<u>VIP User and Web Service APIs and Integrations</u>

- **VIP User and Web Service APIs –** These Service APIs fall under five categories. Each handle different operations necessary for Customer to authenticate their End Users with a strong second factor:

  Management APIs – These APIs allow Customer to create and/or associate a new Authenticator with their VIP account. They also allow Customer to add, update, or delete a user or groups of users with the Service. They allow Customer to assign, update, or remove an Authenticator to an End User, and send an OTP to an End User. These also let Customer manage the state of Authenticators.

  Query APIs – These APIs allow Customer to obtain information about Authenticators as well as End Users, such as when a user was created in VIP, when an Authenticator was last bound to the user, when the user was last authenticated, etc.

  Authentication APIs - These APIs allow Customer to authenticate an Authenticator, or an End User based on verification of proof

of possession of their Authenticator, evaluate the users risk and denying or confirming authentication based on the risk information.

Policy APIs – These APIs allow Customer to set policies that control the behavior of the Service as it relates to End Users and Authenticators

Reporting APIs - Significant events are recorded by Broadcom on a transaction-by-transaction basis. Broadcom maintains audit records independently in multiple media depending upon the sensitivity of the event. Audit trails are created for all management, query, and authentication transactions. These APIs allow the Relying Party to obtain these audit records.

- **VIP Login –** VIP Login provides strong authentication using industry standard federation protocols. Integrating using VIP Login with the Service provides a flexible, standard means for securely authenticating End Users to common web applications that support federated identities.

- **VIP Intelligent Authentication –** VIP Intelligent Authentication builds a risk profile for login events and generates a risk score by analyzing End User's device profile, behavioral patterns, location, network connection and other factors. Depending on the risk associated with a particular login event, Customer can "step up" authentication using out-of-band or two-factor authentication techniques supported within the enterprise or through the Service.

VIP Manager

VIP Manager is a web-based portal, hosted by Broadcom, for the configuration and management of the Service. Customer is given access to this portal for the purposes of configuring Service parameters, viewing reports, and managing End Users and Authenticator Lifecycle Functions. In addition, VIP Manager keeps audit logs that record functions executed by individual Administrators. Access to VIP Manager is controlled by validating either: (i) the Administrator's email address, password, and VIP Authenticator, or (ii) the Administrator's enterprise username and password through a single sign-on functionality enabled by either the VIP Enterprise Gateway or an enterprise-hosted SAML-compliant federation server, in addition to validating the Administrator's VIP Authenticator.

VIP Self Service Portal

VIP Self Service Portal is a web-based portal, hosted by Broadcom, for End Users' VIP Authenticator Lifecycle Functions-related services. Customer can grant direct access to this VIP Self Service Portal to their End Users. Access to the VIP Self Service Portal is controlled by validating an End User's enterprise username and password through a single sign-on functionality enabled by either the VIP Enterprise Gateway or an enterprise- hosted SAML-compliant federation server.

My VIP

My VIP is a web-based portal, hosted by Broadcom, for End Users' VIP Authenticator Lifecycle Functions-related services. This portal is meant to be similar in functionality to VIP Self Service Portal but enables different user flows for End User onboarding. Customer can integrate with My VIP in the same manner as with VIP Self Service Portal.

Audit Trails and Audit Data Retention

Significant events are recorded by Broadcom on a transaction-by-transaction basis. Broadcom maintains audit records independently in redundant media and locations depending upon the sensitivity of the event. Audit trails are created for all authentication, query, and management transactions, and End User self-service and Administrator operations.

All audit information is maintained for 12 months from the time of event for online retrieval, and for up to 7 years for retrieval upon request.

Service Software Components

This Service includes the software components listed below, which should be used only in connection with Customer's use of the Service during the Subscription Term.

Customer must remove service software components upon expiration or termination of the Service.

Any maintenance/support purchased for the Service shall also apply to Customer's use of the Service Software Components.

Customer's use of the following software is optional.

- **VIP Enterprise Gateway –** This is a 'self-hosted' software component deployed by Customer. It may be provided for the integration of enterprise applications and directories. VIP Enterprise Gateway enables multi-factor authentication by utilizing a first and layering multiple second factors of authentication. The first factor can be a password associated with each End User, which is stored in the enterprise directory. The second factor can be one of the many Authenticators as supported by the Service. The second factor validation is performed by the Service. For each validation request sent to the VIP Enterprise Gateway, the first-factor validation is performed locally at the enterprise directory. VIP Enterprise Gateway then completes the second factor authentication against the Service. VIP Enterprise Gateway also records audit logs that record authentication events that are processed through it.

  The Service also includes documentation and custom plug-ins (where necessary) that layer multi-factor authentication on top of many popular enterprise applications that require End User access.

  The respective documentation and custom plug-ins (where necessary) are distributed on-line. The website is updated on a regular basis with new integrations.

- **VIP Access Software Authenticators (for Mobile and Desktop) –** VIP Access is a software Authenticator that is made available to Customer's End Users. This software is an application that is compatible with various mobile and personal computer operating systems. VIP Access offers End User the capability to authenticate to the Service using an OTP or a VIP Push, where available.
- **VIP Mobile Software Development Kit (SDK) -** The VIP Mobile Software Development Kit, sometimes referred to as the Credential Development Kit (CDK), is a software development kit for iOS and Android mobile operating systems. The SDK is typically useful for mobile application developers who prefer to add VIP second factor authentication, transaction signing, and risk-based authentication capabilities to their custom mobile application.
- **VIP Authentication Hub –** VIP Authentication Hub is a cloud-native authentication service that provides orchestrated strong authentication policies combined with the use of Intelligent Authentication risk analysis. It is deployed into a kubernetes cluster and can be integrated with the VIP SaaS service along with other Symantec solutions. It can connect to an LDAP or SCIM identity store and provides SAML and OIDC Provider functionality.

Service Hardware Components

- The Service is compatible with the hardware components noted above.

  Hardware Authenticators may be purchased for an additional fee as a corollary to the VIP Authentication Service.

2: Customer Responsibilities

Broadcom can only perform the Service if Customer provides required information or performs required actions, otherwise Broadcom's performance of the Service may be delayed, impaired or prevented, and Customer may lose eligibility for any Service Level Agreement

- Setup Enablement: Customer must provide information required for Broadcom to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Broadcom in delivery of the Service.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the applicable Transaction Document within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Subscription Term. Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the VIP Manager and VIP Enterprise Gateway, as 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 are entirely in Customer's control, therefore, Broadcom 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.

Validation & ID Protection (VIP) Service

SaaS Listing

- Installation of Service Enabling Software may be required for enabling certain features of the Service.
- Customer is responsible to obtain all necessary End-User and VIP Authenticator information and securely transmit requests to Broadcom to validate VIP Authenticator information and coordinate the activation of VIP Authenticators and their association to End Users. For Authenticators where Broadcom does not explicitly enforce End User to agree to a license agreement, Customer shall require End User to agree to terms and conditions of VIP Authenticator usage in a form substantially similar to the form provided by Broadcom in the "End User Agreement," available at https://www.broadcom.com/company/legal/licensing.
- Customer is responsible to promptly disable or deactivate any VIP Authenticator:
    - upon fraudulent or suspected fraudulent use;
    - upon notification, that the VIP Authenticator has been lost or stolen; or
    - upon request from its End User.
- Customer is responsible for informing Broadcom:
    - of fraudulent or suspected fraudulent use of a VIP Authenticator; or
    - upon notification from End User that their VIP Authenticator has been lost or stolen

3: Entitlement and Subscription Information

Charge Metrics

The Service is available under one of the following Meters as specified in the Transaction Document:

- Per **User,** which means Customer's employees, contractors and external users who are authorized by Customer to use the Services on behalf of Customer. A User's digital identity is represented in the Service as an identifier, either pseudonymous or non-pseudonymous. The Service provides functions to associate one or more Authenticators to a User for ongoing management and verification that they continue to remain under the User's control. They are also sometimes referred to as "End Users" in various Authenticator Lifecycle Functions.
- Per **Authenticator**. Authenticators are also sometimes referred to as "Credentials" in various Authenticator Lifecycle Functions and for billing and invoicing purposes. Authenticators are associated with Users in the Service. (For more information, please refer to Section 1)

The Service limits the number of Authenticators associated with each User. In addition, who is a "User" or what is an "Authenticator," and their associated usage quantity may be determined by Broadcom at its sole discretion.

User-based licensing is based on the count of "Active Users." An Active User is defined as a user identity in the Service that has used some capability of the Service in the last 12-month period. This could include authenticating using a credential, evaluating the user risk score, or registering or removing credentials associated with the user, among other activities. The User's 'last activity' date is stored on the User identity record. Credential-based licensing is based on the count of "Active Credentials". An Active Credential is a credential in the Service that has been validated in the last 12-month period. The 'last validated' date is stored on the credential record.

4: Customer Assistance and Technical Support

Customer Assistance

Broadcom 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

Validation & ID Protection (VIP) Service

SaaS Listing

Technical Support

If Broadcom is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support for Services will be performed in accordance with the published terms and conditions and technical support policies published in the "Broadcom Software Maintenance Policy Handbook" at https://support.broadcom.com/external/content/release- announcements/CA-Support-Policies/6933.

Maintenance to the Service and/or supporting Service Infrastructure

Broadcom must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit https://status.broadcom.com/. 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. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Broadcom will provide seven (7) calendar days' notification.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Broadcom will provide a minimum of one (1) calendar day notification. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Broadcom will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, Broadcom will provide fourteen (14) calendar days' notification. Broadcom may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

5: Additional Terms

Broadcom may modify the Service and/or the corresponding SaaS Listings at any time: (a) due to changes in applicable laws or industry standards; and (b) for any other reason, if the modification does not materially reduce the level of performance, functionality, security or availability of the Service during the Subscription Term.

- Customer must present the terms of the Agreement to End Users and must make reasonable efforts to notify Broadcom of any known breach of such terms.
- If Broadcom determines that Customer's aggregate activity on the Service imposes an unreasonable load on bandwidth, infrastructure, or otherwise, Broadcom may impose controls to keep the usage below excessive levels. For Inline Service the expected average usage per week is 20 transactions per User or Authenticator and the expected peak usage is 10 transactions per second for Customer. Upon receiving notification (e.g., email) of excessive (vs. expected) usage, Customer agrees to remediate their usage within ten (10) days, or to work with Broadcom or its reseller to enter into a separate fee agreement for the remainder of the Subscription Term. If the parties are not able to establish a resolution within ten (10) days after the initial notification, then Broadcom may institute controls on the Service or terminate the Service and the Agreement, without liability. In addition, if Broadcom determines that the excessive usage may present a risk to the Service, Broadcom may implement technical and business measures to bring usage into compliance.
- The Service does not include Customer's configurations, policies and procedures implemented and set by Customer that are available through the Service. Customer is solely responsible for selecting their configurations and assuring that the selection conforms to policies and procedures and complies with all applicable laws and regulations in jurisdictions in which Customer is accessing the Service.
- Customer and its End users, if utilizing VIP SMS OTP, are advised of the following:

  (i) Symantec Validation & ID Protection, as described in this SaaS Listing, is provided according to the terms and conditions herein, any other terms referenced on the Broadcom quote or other transaction document herein, any other terms referenced on the Broadcom quote or other transaction document through which you obtained a license for the Service, and the Broadcom Privacy policy located at https://www.broadcom.com/company/legal/privacy/policy;
  (ii) Message and data rates may apply;

(iii) Message frequency varies;
(iv) Using the VIP SMS OTP is optional. End Users who reply "STOP" will stop receiving SMS messages. End users who reply "HELP" will be directed to the following support assistance: technical.support@broadcom.com or 800-225-5224;
(v) Carriers are not liable for delayed or undelivered messages.
Customers must advise End Users that they may incur additional charges from their wireless carriers and that End Users are solely responsible for such charges when sending and/or receiving any SMS text messages or voice calls, including the SMS text messages and voice calls issued as part of this Service. Broadcom is not responsible to reimburse Customer or End Users for such charges including, but not limited to, inter-connection, access, termination, pager, wireless, landline or any phone charges in the provision of this Service.

- When validating a VIP Authenticator within VIP, Broadcom only determines that the VIP Authenticator is valid and active, and that the OTP value generated from the VIP Authenticator or response to VIP Push is associated with the VIP Credential ID. Broadcom makes no representations about VIP Authenticators not supplied by Broadcom and is not responsible for damages relating to the use of any VIP Authenticator outside its control.

- **No Service Carry-over.** Any units of the Service which are not consumed during the annual period for which such units were purchased may not be carried over to a subsequent annual period whether or not during the same Subscription Period.
- **Termination Due to End of Service Availability.** The Service (or a portion) may be terminated upon ninety (90) days prior written notice by Broadcom, in the event that the Service (or a portion) are affected by Broadcom's cessation of, or designation of 'end of life' of, such Service (or a portion).

6: Definitions

Capitalized terms used in this SaaS Listing, and not otherwise defined in the Agreement or this SaaS Listing, have the meaning given below:

"**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.

"**Authenticator Lifecycle Functions**" means the primary management functions related to the lifecycle of any VIP Authenticator, including, activation/deactivation, locking/unlocking, disabling/enabling and synchronization.

"Credit Request" means the notification which Customer must submit to Broadcom through their sales representative or by contacting Broadcom Customer Support to request a credit.

"**Customer**" means the entity that purchased the Service, including any agents and/or contractors it authorizes to install and use the Service on its behalf.

"**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 Broadcom that a credit is due to Customer.

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

Validation & ID Protection (VIP) Service

SaaS Listing

Exhibit-A

Service Level Agreement(s)

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this SaaS Listing only. If Broadcom does not achieve these SLA(s), then Customer may be eligible to receive a Service Credit. Service Credits are Customer's sole and exclusive remedy and are Broadcom sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline Service, and ii) Non-Inline Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the ability of End User to authenticate using the Service. Inline Services include all APIs and components that allow provisioning, query, validation and management of Authenticators and Users. This includes multi-page UI components such as Authentication JavaScript and VIPLogin.

Inline Service Availability	**≥99.95%**

- **Non-inline Service Availability** is access to the portals and APIs that govern the features of the Service that do not impact business continuity of Customer and the authentication of end-user to the Internet (e.g., reporting tools used by the Administrator). Examples of Non-Inline Service for VIP is any portal that provides management and reporting applicable to VIP including VIP Reporting APIs, VIP Manager, VIP Self Service portal and My VIP.

Non-Inline Service Availability	**≥99.9%**

b. Other SLAs:

- **Out of Band Delivery Services**: Out-Of-Band delivery services is any service which Broadcom provides to deliver one-time passwords or other forms of actionable notifications to End User. SMS text messages, Voice calls and Push notifications are examples of Out- Of-Band delivery services.

Out of Band Delivery Service	**≥99.9**

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of 100% total minutes per calendar month as follows:

$$\frac{\text{Total Minutes in Calendar Month} - \text{Excused Outages} - \text{Non-Excused Outages*}}{\text{Total} - \text{Excused Outages}} \times 100 > \text{Availability Target}$$

**Non-Excused Outages = Minutes of Service disruption that are not an Excused Outage*

Note: The availability calculation is based on the entire calendar month regardless of the Service start date.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Customer's account.

Broadcom will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24 hour period. A Customer may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Service Credits:

- May not be transferred or applied to any other Broadcom Online Service, even if within the same account.

- Are the only remedy available, even if Customer is not renewing for a subsequent term. A Service Credit is added to the end of Customer's current Subscription Term.
- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Customer may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Customer must submit the claim in writing via email to Broadcom Customer Support. Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for Broadcom to review the claim. Each claim must include the following information:

(i) The words "Service Credit Request" in the subject line.
(ii) The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
(iii) An explanation of the claim made under this SaaS Listing, including any relevant calculations.

All claims will be verified against Broadcom's system records. Should any claim be disputed, Broadcom will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Customer.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

- Planned Maintenance and Unplanned Maintenance as defined in the SaaS Listing.
- Force Majeure as defined in the Agreement.
- Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

- Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
- Customer has not paid for the Service.
- Third party, non-Broadcom branded products or services resold with the Service.
- Hardware, software or other data center equipment or services not in the control of Broadcom or within the scope of the Service.
- Any item that is not a Service Component that is provided for use with the Service.
- Technical support provided with the service.
- Failure of Customer to correctly configure the Service in accordance with this SaaS Listing.
- Hardware or software configuration changes made by the Customer without the prior written consent of Broadcom.
- Unavailability of a specific web page or a third party's cloud application(s).
- Individual data center outage.
- Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
- Failure of Customer's internet access connections.
- Suspension and termination of Customer's right to use the Service.
- Alterations or modifications to the Service, unless altered or modified by Broadcom (or at the direction of or as approved by Broadcom
- Defects in the Service due to abuse or use other than in accordance with Broadcom's published Documentation unless caused by Broadcom or its agents.
- Customer-requested hardware or software upgrades, moves, facility upgrades, etc.

Service-specific exclusions: VIP SLAs will not operate: (i) in respect of facilities, networks, connectivity and other acts of third parties not under Broadcom's control, including wireless carriers, private entities, government entities, and the like ("SMS Network", "Telephone Network", remote notification systems). Broadcom shall not be liable for any interruption, delay, suspensions, and other acts and/or omission by such third parties that are not within Broadcom's control.

END OF EXHIBIT A