

schedule 2n

additional terms for MessageLabs services

1. SERVICE DESCRIPTION

MessageLabs service provides an internet-level e-mail content filtering.

2. DEFINITIONS

“**Bulk Email**” means a group of more than five hundred (500) E-mail messages with substantially similar content sent or received in a single operation or a series of related operations;

“**Documentation**” means documentation provided by Interoute including, but not limited to, specifications for the Service;

“**Email**” means any SMTP message sent or received via the Service;

“**Service**” means the provision and supply of an internet-level e-mail content filtering service as described in this Schedule;

“**Open Relay**” means an Email server configured to receive Email from an unknown or unauthorised third

party and forward the Email to one or more recipients that are not users of the Email system to which that Email server is connected. Open Relay may also be referred to as “spam relay” or “public relay”;

“**Service Commencement Date**” means the date when the Service is made available to the Customer;

“**User**” means a person or mailbox on behalf of which Email is being scanned by the Service; and

“**Virus**” means a piece of program code, including a self-replicating element, usually (but not necessarily) disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is designed so that it may infect other computer systems.

Any other capitalised terms have the meanings set out in Interoute’s Standard Terms and Conditions.

3. PROVISION OF SERVICES

- 3.1 Subject to the prior written acceptance by Interoute of a Purchase Order placed by Customer, Interoute shall provide the Services to the Customer in accordance with the terms of this Agreement. The Services shall not be made available to the Customer for a minimum of seven (7) days from the date of acceptance of the relevant Purchase Order or Change Order by Interoute.
- 3.2 Interoute will provide the Service with reasonable skills, care and diligence and in accordance with the industry standards and the relevant Interoute Service specifications contained in the Appendixes hereto.
- 3.3 Without prejudice to the rights under this Agreement and under law, the remedy of the Customer under clause 3.2 above shall be Interoute’s obligation, if any, to repeat the Service or if Interoute is unable or unwilling to repeat the Service, Interoute will refund the amount paid by the Customer during the previous month for the actual Service in breach of clause 3.2 above. Interoute shall have no additional liability to the Customer.
- 3.4 Interoute reserves the right both prior to the provisioning of the Service and at any time during the supply of the Service to test whether the Customer’s Email system(s) allow Open Relay. If at any time the Customer’s Email systems are found to allow Open Relay, Interoute reserves the right to immediately withhold provision of or suspend all or part of the Service to the Customer until the problem has been resolved.

schedule 2n

additional terms for MessageLabs services

- 3.5 If at any time any Customer's Email system(s) are found to be used for Bulk Email, Interoute will inform Customer and reserves the right to immediately withhold the provision of or suspend part or all of the Service to the Customer until the problem has been resolved.
- 3.6 If at any time the provision of the Service to the Customer would compromise the security of the Service due, without limitation, to hacking attempts, denial of service attacks, mail bombs or other malicious activities either directed or originating from the Customer's domains, Interoute may temporarily suspend the provision of the Service to the Customer. In such case, Interoute will inform the Customer (prior to or after the suspension) and will work with the Customer to resolve such issues. Interoute shall use its reasonable endeavours to re-instate Service to the Customer as soon as practicable.
- 3.7 Subject to the applicable legislation, Interoute may provide the Service from any hardware installations forming part of the Service anywhere in the world and may, at any time, transfer the provision of the Service from one installation to another. Interoute does not guarantee that any such installation, or part thereof, is dedicated to the sole use of the Customer.

4. CUSTOMER'S OBLIGATIONS

- 4.1 The Customer undertakes and agrees, at all times throughout the Term of this Agreement:
- 4.1.1 not to re-sell, sub-lease, sub-rent or sub-license the Service;
 - 4.1.2 to test its Email system(s) to ensure they do not support Open Relay prior to placing any order for the Service;
 - 4.1.3 to ensure its Email system(s) are not being used to send Bulk Email or unsolicited commercial Email, also known as "spam";
 - 4.1.4 to obtain and promptly pass to Interoute, at least seven (7) Working Days prior to the scheduled commencement of the Service, all relevant technical and related information, complete with any consents required from the Customer or any third party, necessary for Interoute to enable and provide the Service;
 - 4.1.5 to have valid and sufficient insurance and bonds as may be required by any applicable law;
 - 4.1.6 to comply with any requirements by Interoute to utilise e-commerce applications (such as web and intra/extranet) for administrative and related activities such as, but not limited to, submission of orders, order processing, issue and updating of Documentation, processes and procedures, support activities, and Service changes;
 - 4.1.7 to use the Service for legitimate business purposes and to comply with all relevant legislation applicable to the use of the Internet; and
 - 4.1.8 not to use the Service for any unlawful purpose or in breach of the laws of England and Wales or the laws from the jurisdiction where the Service is provided, or any other law applicable to the use of the Internet. Customer acknowledges that prohibited uses include, but are not limited to:
 - a. civil or criminal offences or copyright and trademark infringement; or
 - b. transmission or display or posting to a bulletin board of obscene, indecent or pornographic material; or
 - c. commission of any criminal offence under the Computer Misuse Act 1990 (or any replacing statute) or any similar legislation in any country; or
 - d. any transmission or display or posting to a bulletin board of any material which is of a defamatory, offensive, abusive or menacing character or which causes annoyance, inconvenience or needless anxiety to any person; or
 - e. transmission or display or posting to a bulletin board of any material in breach of the Data Protection Act 1998 (or any replacing statute) or any other similar legislation in any other country; or
 - f. transmission or display or posting to a bulletin board of any material in breach of any confidentiality obligations or of a trade secret; or

schedule 2n

additional terms for MessageLabs services

- g. use the Service in any manner which is in violation or infringement of the rights of any individual, organisation or company in the United Kingdom and/or elsewhere.

4.2 Customer hereby indemnifies and will keep Interoute, its employees, officers, agents, affiliates and sub-contractors, fully and effectually indemnified on demand from any and against all direct actions, claims, losses, liability, proceedings, damages, costs, expenses (including reasonable legal costs and expenses) suffered or directly incurred by Interoute and arising directly or indirectly out of any claim made against Interoute due to the breach by the Customer of clauses 4.1.7 and 4.1.8 above.

5. CHARGES AND PAYMENT

5.1 Interoute will commence charging for the Service from the Service Commencement Date. Charges for the Service shall relate to both the number of Users and domains being scanned by the Service (the "Registered Usage"). The charge(s) initially payable by the Customer shall relate to the Registered Usage declared by the Customer upon ordering the Service, and such Registered Usage shall be subject to change in accordance with clause 5.4 below.

5.2 Interoute shall charge the Customer in relation to:

5.2.1 Users: monthly charge per User, as set out in the Order Form; and

5.2.2 Domains: a charge, as set out in the Order Form, shall apply, at any time, to any of the following: (i) domains being added to the Service, (ii) changes to such domains, and (iii) domains being removed from the Service.

5.3 The minimum number of Users per Customer supported by the Service is twenty five (25). Registered Usage shall be equal to twenty five (25) or multiples of twenty five (25) Users and any number of domains.

5.4 Customer must notify Interoute in writing if, at any time, the number of Users or domains being scanned exceeds or is likely to exceed the Registered Usage and Interoute will increase the Registered Usage accordingly. Additionally, Interoute will monitor Customer's actual usage of the Service and, in the event that that actual number of Users or domains being scanned exceeds the Registered Usage, Interoute will increase the Registered Usage accordingly. In the event of any increase of the Registered Usage, Interoute will, at its sole discretion, raise additional invoices and/or make the necessary adjustments to subsequent invoices to cover charges for the increase in Registered Usage on a pro-rata basis for the remaining part of Customer's current invoicing period.

5.5 Interoute shall have the right to increase the charges applicable to the Service upon thirty (30) days notice to the Customer. Interoute may also decrease any of the charges at any time without notice.

5.6 Interoute shall invoice the Customer on a monthly basis for the charges applicable to the Service. Customer shall pay the invoices in full within thirty (30) days from the date of the invoice. All payment shall be made via wire transfer in pounds sterling, unless otherwise set out in the Order Form, in immediately available funds.

5.7 All the charges shown for the Service are exclusive of any Taxes. Such Taxes will be payable by the Customer and added to any invoice for the Service at the then current rate at the date of the invoice.

5.8 Any and all expenses, costs and charges incurred by the Customer in the performance of any or all of its obligations under this Agreement shall be borne in full by the Customer.

schedule 2n

additional terms for MessageLabs services

5.9 Customer shall under no circumstances be entitled to any set-off, counter-claim, abatement or other similar deduction to withhold payment of any amount due to Interoute. All payments are non-refundable, unless such payment is subject to a bona fide dispute. In the event of a dispute, Interoute records shall prevail except in cases of manifest error.

6. TERM AND TERMINATION

6.1 Each Purchase Order for the Service shall have a minimum term of twelve (12) months (the "Minimum Term") and, upon expiration of the Minimum Term, shall automatically continue in force until terminated by either Party giving not less than three (3) months prior written notice to the other Party. Such notice may expire on or after the Minimum Term.

6.2 Notwithstanding clause 2.4 of Schedule 1 of the Master Agreement, Interoute reserves the right to suspend the provision of the Service to the Customer, at any time and with immediate effect, in the event that:

6.2.1 The Customer is sending Bulk Email through the Service;

6.2.2 The Customer allows Open Relay to occur in any of its Email system(s) using the Service; or

6.2.3 The provision of the Service would compromise the security of the Service as set out in clause 3.6 above.

6.3 Upon termination of this Agreement or any Purchase Order placed under this Schedule, all invoices shall become due and payable.

6.4 Termination of this Agreement shall not itself give rise to any liability on the part of Interoute to pay any compensation to the Customer for loss of profits or goodwill.

7. LIABILITY

7.1. Interoute liability to the Customer for recoverable loss or damage to the Customer's tangible property, caused either by:

a. defects in the Service resulting from Interoute's negligence, or

b. the negligence of Interoute's employees, officers, agents, affiliates and sub-contractors,

is limited to a maximum of (i) three hundred thousand pounds sterling (£300,000), or the amount actually paid by the Customer to Interoute hereunder for the Service during the four (4) months immediately prior to the event causing such loss. Such limit shall apply to each event or series of connected events. For the avoidance of doubt data does not constitute tangible property.

7.2. Interoute liability to the Customer for actual loss by the Customer caused either by;

a. defects in the Service resulting from Interoute' negligence, or

b. the negligence of Interoute' employees, officers, agents, affiliates and sub-contractors,

is limited to a maximum of the actual amount paid by the Customer to Interoute for the Service provided to the Customer suffering such loss during the four (4) months immediately prior to the event causing such loss. Such limit shall apply to each event or series of connected events.

7.3. Subject to Clauses 10.5 of Schedule 1 of this Agreement and 4.2 of this Schedule, neither party accepts any liability under or in relation to this Agreement or its subject matter (whether such liability arises due to negligence, breach of contract, misrepresentation or for any other reason)

schedule 2n

additional terms for MessageLabs services

for any loss of profits, loss of sales or turnover, loss of or damage to reputation, loss of contracts, loss of customers, loss of, or loss of use of, any software or data, loss of use of any computer or other equipment or plant, wasted management or other staff time, losses or liabilities under or in relation to any other contract, indirect loss or damage, consequential loss or damage, loss(es) directly or indirectly due to network access by third parties; or special loss or damage. For the purposes of this Clause 7.3 the term "loss" includes a partial loss or reduction in value as well as a complete or total loss.

7.4. Subject to Clauses 10.5 of Schedule 1 of the Contract, Clauses 4.2, 7.1, 7.2 and 9.2 of this Schedule, Clause 5.2 of Appendix 1 Part A below, Clause 5.1 of Appendix 1- Part B below, and Clause 7.1 of Appendix 1 – Part C below, either party's liability, in any consecutive twelve (12) month period, whether in contract, tort or otherwise, howsoever arising out of or in connection with this Agreement shall be limited to one hundred and twenty percent (120%) of the total price paid by the Customer for the Service for the twelve (12) months immediately prior to the event causing such loss per event or series of connected events.

8. INTELLECTUAL PROPERTY

The Intellectual Property Rights in the Service and any hardware or software Interoute uses in connection with the Service is and will at all times remain the sole property of Interoute or that of relevant licensor(s). Customer shall acquire no rights, title or interest whatsoever in any Intellectual Property Rights contained in the Service.

9. DATA PROTECTION

9.1 Customer shall comply with any applicable laws and regulations in respect of data protection and privacy (including but not limited to the Data Protection Act 1998, or any replacing statute). Customer acknowledges that Interoute has no control or influence over the content of the Emails processed by the Service. Customer shall indemnify and hold Interoute harmless for any claims from any third parties (including but not limited to Customer's employees, officers, agents, affiliates and sub-contractors and governmental agencies) arising out of any breach of such laws and regulations.

9.2 Customer shall inform any person who uses any communications system covered by the Service, that communications transmitted through such system may be intercepted, and indicate the purposes of such interception. Customer shall hold Interoute harmless from any claims from a third party (including but not limited to Customer's employees, officers, agents, affiliates and sub-contractors and governmental agencies) relating to such interceptions. Customer shall not use, or require Interoute to use, any data obtained via the Service for any unlawful purposes.

Appendix 1 Service Description

1. Introduction

- 1.1 The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis. The Service is monitored for hardware availability, service capacity and network resource utilisation. Through stringent monitoring of service levels, regular adjustments are made to the Service to ensure its optimum efficiency is maintained.
- 1.2 The Service is available to Customers whose Email systems are permanently connected to the Internet with a fixed IP address. It cannot be provided to Customers whose Email systems are connected to the Internet via dial-up or ISDN lines or whose IP address is dynamically allocated.

2 Management

- 2.1 Interoute continuously monitors Email queue lengths. If a rising Email queue is detected for a connected domain, Interoute will test for the ability of the receiving mail server to receive Email. If this test fails, the affected party will be notified. If Interoute is unable to deliver Email to the Customer's mail server, Interoute will store the Customer's inbound Email for up to seven (7) days pending delivery.
- 2.2 Wherever possible, planned maintenance will be carried out without affecting the Service. This will generally be achieved by carrying out planned maintenance during periods of anticipated low Email traffic and by carrying out planned maintenance on part, not all, of the network at any one time. During planned maintenance periods the Email traffic may be diverted round sections of the network not undergoing maintenance in order to minimise disruption to the Service.
- 2.3 Where emergency maintenance is necessary and is likely to affect the Service, Interoute shall endeavour to inform the affected parties and will post an alert message on InSight as soon as possible and in any case within one (1) hour of the start of the emergency maintenance.

3 InSight

An integral part of the Service is the internet-based configuration, management and reporting tool called InSight. InSight is made available to the Customer via a secure password protected login which should not be disclosed to a third party. InSight provides the facility for the Customer to view data and statistics on their use of the Service and offers a number of configuration and management facilities.

4 Technical Support

- 4.1 Interoute will on a twenty-four (24) hours/day by seven (7) days/week basis:
 - a) provide technical support to the Customer for problems with the Service; and
 - b) liaise with the Customer to resolve such problems.

5 Customer Service

- 5.1 Interoute will provide customer service during Working Hours to:
 - a) receive and process orders for provisioning the Service;
 - b) receive and process requests for modifications to the operational aspects of the Service; and
 - c) respond to billing and invoicing queries.
- 5.2 On receipt of a fully completed and actionable order or Service Change Request, the Interoute customer service team will aim to provision the Service within three (3) Normal Working Days, providing all the phases of technical due diligence have been completed.

Appendix 1 – Part A The Anti-Virus Service

1. Overview

- 1.1 The Anti-Virus service (“AV”) is Interoute’ internet-level Email Virus scanning service. The Customer’s inbound and outbound Email including all attachments, macros or executables are directed through the AV service using DNS and MX record settings.
- 1.1 Email and attachments are electronically routed via Control Towers and digitally examined. The Email and attachments are scanned by multiple industry leading anti-virus products including the scanner, Skeptic™.
- 1.2 The Service will scan as much of the Email and its attachments as possible. It may not be possible to scan attachments with content which is under the direct control of the sender (for example, password protected and/or encrypted attachments). Such Email and/or attachments are excluded from the 100% Service Level in Appendix 2.

2 Alert Messages

- 2.1 If a Customer’s inbound Email or attachments are found to contain a Virus, an automatic alert may, if selected by the Customer, be despatched to the sender and intended recipient by way of notification. With a Customer’s outbound Email the Service may notify the sender only and not the intended recipient. User notifications may also be sent to an Email administrator in both cases. The infected Email is forwarded to a secure server pending automatic destruction after thirty (30) days, provided that it is not transported as a mass mailer virus, in which case it will be deleted immediately.
- 2.2 In the case of a major breakout of a new Virus, an alert message will be posted on InSight.

3 Configuration

- 3.1 InSight can be used for customising banner texts, releasing Virus-infected Email and setting maximum Email sizes.

4 Releasing a Virus-Infected Email

- 4.1 Where a Virus-infected Email is shown to be releasable, it can be released from the secure server using InSight. The Email will be released either to the first address of the original recipient list or to a specified address previously notified to Interoute and logged by Interoute in InSight (Note: these addresses may be group Email names or aliases in which case the Email will be released to all addressees in the group or alias). Optionally the Virus-infected Email may be released to an alternative address by Interoute on receipt of the appropriate Release Authorisation Form. Interoute will only act on requests authorised by Customers to forward Virus-infected Email. Interoute will not return Virus-infected Email to the sender. Interoute will not forward Virus-infected Email to third parties. Certain Virus-infected Emails sent to the customer are not releasable due to them containing a Virus which is particularly infectious or damaging. These are shown on InSight as being not releasable.

5 AV Terms and Conditions

- 5.1 Viruses released as described in Clause 4.1 above of this Appendix shall be excluded from any Service Level and/or liquidated damages as described in the Service Level in Appendix 2.
- 5.2 The Customer agrees to indemnify Interoute against all and any losses, costs and expenses Interoute may incur as a result of the intentional release of a Virus-infected Email under Clause 4.1 above.
- 5.3 If requested to release a Virus-infected Email, Interoute will release it within eight (8) Working Hours of receipt of a duly authorised release request.

Appendix 1 – Part B The Image Control Service

1. Overview

- 1.1 The Image Control service ("IC") is Interoute' internet-level Email anti-porn service which is designed to detect pornographic images contained in image files. IC is part of the portfolio of services managed on a twenty-four (24) hours/day by seven (7) days/week basis.

2 Service Description

- 2.1 The Customer's inbound and outbound Email can be scanned using Image Composition Analysis (ICA) for pornographic images contained in image files attached to Email.
- 2.2 If a Customer's inbound or outbound Email is suspected to contain a pornographic image, one of a number of actions will be taken depending on the configuration options selected by the Customer.

3 Configuration

- 3.1 On receipt of a fully completed and accepted order, Interoute will enable IC for the Customer. Initially IC will be enabled for each of the Customer's domains. The Customer is responsible for setting the configuration options for IC for each domain according to the Customer's needs. The Customer configures IC using InSight.
- 3.2 Options are available for specifying the level of detection sensitivity. Sensitivity can be set to High, Medium or Low. These settings are particularly subjective, however, as a guide more images will be suspected to be pornographic at High sensitivity and fewer images will be suspected to be pornographic at Low sensitivity.
- 3.3 Options are available for defining the actions to be taken on detecting a suspected pornographic image. These options may be set independently for inbound and outbound Email and should be set in line with the Customer's existing Acceptable Computer Use Policy (or its equivalent). These options are:
- 3.3.1 log suspected Email (provides statistics viewable via InSight)
 - 3.3.2 tag suspected Email within the header (for inbound Email only)
 - 3.3.3 copy suspected Email to a pre-defined Email address
 - 3.3.4 redirect suspected Email to a pre-defined Email address
 - 3.3.5 delete suspected Email.

4 Reporting

- 4.1 If the chosen options in Clause 3.3 of this Appendix 1 – Part B are to redirect or delete Email containing a suspected pornographic image, then an automatic alert will be despatched to the sender. If the Email is inbound to the Customer an automatic alert is also sent to the intended recipient.
- 4.2 Reporting on the effectiveness of IC is provided through InSight where statistics are available on the numbers of inbound and outbound Emails suspected of containing pornographic images. InSight may be configured to generate reports which are sent by Email to the Customer on a weekly or monthly basis.

5 IC Terms and Conditions

- 5.1 NO PORNOGRAPHIC IMAGE DETECTION SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE MESSAGELABS CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM

schedule 2n

[additional terms for MessageLabs services](#)

ANY FAILURE OF THE SERVICE TO DETECT A PORNOGRAPHIC IMAGE OR FOR WRONGLY IDENTIFYING AN IMAGE AS SUSPECTED TO BE PORNOGRAPHIC WHICH PROVES SUBSEQUENTLY NOT TO BE SO. Furthermore the Customer agrees to indemnify Interoute for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any suspected pornographic or non-pornographic image except where such claim arises due to Interoute breach of contract or negligent act or omission.

- 5.2 It may not be possible to scan attachments with content which is under the direct control of the sender (for example, password protected and/or encrypted attachments).
- 5.3 IC is not able to scan for pornographic images embedded in other documents.
- 5.4 Interoute emphasises that the configuration of IC is entirely in the control of the Customer. IC is intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel and so Interoute advises the Customer to always check their local legislation prior to deploying IC. Interoute can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of IC. The Customer recognises that the definition of what does and what does not constitute a pornographic image is subjective. The Customer should take this into consideration when configuring the Service.
- 5.5 If the Customer releases or requests the release of a Virus-infected Email, the released Email will not be scanned by IC prior to release.

Appendix 1 – Part C The Anti-Spam Service

1. Overview

- 1.1 The Anti-Spam service (“AS”) is Interoute’ internet-level Email Anti-Spam service which is designed to protect the Customer from unsolicited or unwanted Email. AS is part of the portfolio of services managed on a twenty-four (24) hours/day by seven (7) days/week basis by Interoute.

2. Service Description

- 2.1 The Customer’s inbound Email may be scanned using a number of different detection methods to determine whether or not it is Spam. If an inbound Email is suspected as being Spam, one of a number of actions will be taken depending on the configuration options selected by the Customer. The configuration options are listed in Clause 3.2 below and are accessible by the Customer through InSight.
- 2.2 A private whitelist may be compiled by the Customer. If this detection method is selected and an incoming Email is received from a whitelisted domain, it will automatically bypass any other selected Spam detection methods.
- 2.3 A private blacklist may be compiled by the Customer. If this detection method is selected and an incoming Email is received from a blacklisted domain an action will be taken as defined by the configuration options in Clause 3.2 below.
- 2.4 A number of public blacklists may be used. If any of these detection methods are selected and an incoming Email is received from a domain listed on one of the selected public blacklists an action will be taken as defined by the configuration option in Clause 3.2 below.
- 2.5 If the Email has not been deleted as a result of being blacklisted as above and the signaturing system is selected and the action that would be taken as a result of detecting the Email as Spam as is more severe than that already selected as a result of blacklist detection, the Customer’s inbound Email is scanned using the signaturing system. If an Email is detected by this method as being Spam then action will be taken as defined by the configuration options in Clause 3.2 below. This action will supersede any less severe action previously allocated by any of the blacklist methods.
- 2.6 If the Email has not been deleted as a result of the preceding processes and heuristics detection is selected and the action that would be taken as a result of detecting the Email as Spam as configured by the Customer is more severe than that already selected as a result of detection by the preceding processes, the Customer’s inbound Email is scanned using heuristics scanning. If an incoming Email is heuristically detected as being Spam action will be taken as defined by the configuration options in Clause 3.2 below. This action will supersede any less severe action previously allocated by any of the preceding methods.
- 2.7 Black/white lists provided by Interoute are given as examples only.

3. Configuration

- 3.1 On receipt of a fully completed and accepted order, Interoute will enable AS for the Customer. Initially AS will be enabled for each of the Customer’s domains. The Customer is responsible for setting the configuration options for AS for each domain according to the Customer’s needs. The Customer configures AS using InSight.
- 3.2 Options are available for specifying the actions to be taken should an Email be suspected as being Spam. These options, listed below, are selectable for each of the available detection methods:
- 3.2.1 tag suspected Email within the header
- 3.2.2 tag suspected Email within the subject line;

schedule 2n

additional terms for MessageLabs services

3.2.3 redirect suspected Email to a pre-defined Email address (which must be on a domain being scanned by the Service);

3.2.4 delete suspected Email;

4. Spam Quarantine Service Description

4.1 If the Customer configures Spam Quarantine for a domain, each User's Spam Quarantine account will be set up automatically upon the first time that suspected Spam is identified by the AS service and the User will automatically receive an Email notification.

4.2 Spam Quarantine is accessed by the User via the Spam Manager interface.

4.3 Suspected Spam can be stored for a maximum of fourteen (14) days after which it will be automatically deleted

4.4 If Spam Quarantine is not able to accept Email the suspected Spam will be tagged and sent to the recipient.

5. Spam Quarantine Configuration

5.1 The Customer configures Spam Quarantine via Insight.

5.2 Default User notifications are set to 5.2.1 below. The User may at any time select one of the following notification options:

5.2.1 Notifications to be received daily;

5.2.2 Notifications to be received at various frequencies;

5.2.3 Notifications not to be received.

5.3 The following release options are available through Spam Manager:

5.3.1 Delete Email;

5.3.2 Release Email to original recipient address;

5.3.3 Review text of Email.

5.4 Through Insight a Customer may control other aspects of Spam Manager: (a) automated or manual notification policy; (b) setup of summary notifications; (c) default language settings; (d) whitelisting requests; (e) preset alias emails and (f) specialised Users (eg Quarantine Administrators).

6 Reporting

Reporting on the effectiveness of AS is provided through InSight. InSight may be configured to generate reports which are sent by Email to the Customer on a weekly or monthly basis.

7 AS Terms and Conditions

7.1 NO ANTI-SPAM SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE MESSAGELABS CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT SPAM OR FOR WRONGLY IDENTIFYING AN EMAIL SUSPECTED AS BEING SPAM WHICH PROVES SUBSEQUENTLY NOT TO BE SO. Furthermore the Customer agrees to indemnify Interoute for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any item suspected as being Spam except where such claim arises due to Interoute breach of contract or negligent act or omission.

7.2 Interoute emphasises that the configuration of AS is entirely in the control of the Customer. Interoute recommends that the Customer has an Acceptable Computer Use Policy (or its equivalent) in place. In certain Countries it may be necessary to obtain the consent of individual personnel and so Interoute advises the Customer to always check their local legislation prior to deploying AS. Interoute can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of AS.

Appendix 2 Service Levels

1. Definitions

1.1. The following words shall have the following meanings for the purposes of this Service Level:

“Credit Request” means the notification which the Customer must submit in written form (either by email to support@Interoute.com unless otherwise notified by Interoute) to Interoute in accordance with the provisions of this Service Level;

“Interoute Tracker” means a tool by which Service Availability and Latency are measured by recording the roundtrip data of an Email that is sent to each tower every 5 minutes;

“Monthly Charge” means the monthly charge payable by the Customer to Interoute for the Service provided to the Customer affected by a breach of this Service Level.

“Planned Maintenance” means periods of maintenance which will cause disruption of Service due to non availability of the Designated Tower Cluster. Interoute shall provide the Customer with seven (7) Working Days prior notification in relation to any Planned Maintenance.

“Service Level” means this Appendix 2;

“Tower” means a cluster of load balanced Email servers.

2. General

2.1. In the event that the Customer believes it is entitled to a remedy in accordance with this Service Level, the Customer shall submit a Credit Request to Interoute within ten (10) days of the end of the month in which the eligibility occurred. Credit eligibility is subject to verification by Interoute’ internal logs and other appropriate documentation as detailed herein. If eligibility for a credit is confirmed by Interoute, Interoute will credit the Customer in accordance with the provisions of this Service Level. The Customer recognises that logs are only kept for a limited number of days and therefore any Credit Request submitted outside of the stipulated timeframe will be deemed invalid.

2.2. This Service Level will not operate: (a) until the Customer has been receiving the Service for 30 days; (b) if the Customer’s system configuration is not compliant with all Interoute standard configuration guidelines as published from time to time; (c) during periods of Planned Maintenance; (d) during periods of non-availability due to Force Majeure or acts or omissions of either the Customer or a third party; or (e) during any period of suspension of service in accordance with the Agreement.

2.3. The remedies set out in this Service Level shall be the Customer’s sole and exclusive remedy in contract, tort or otherwise in respect of levels of Service.

2.4. All credits will be pro rated to the number of Users affected by the degradation in levels of Service.

2.5. The maximum accumulative liability of Interoute in any calendar month shall be no more than 100% of the Monthly Charge paid by the Customer.

3. Email Service Availability

3.1 This Email Service Availability SLA will only operate if the Customer utilises one or more of the Email Services.

3.1 “Designated Tower Cluster” means a cluster of Towers, minimum of two, designated to provide the Email Services to the Customer.

schedule 2n

additional terms for MessageLabs services

- 3.2 "Email Service Availability" means an ability to establish a SMTP session on port 25 of the Designated Tower Cluster with the ability to transmit an Email in that;
- 3.2.1 In relation to the Customer's inbound Email it is the availability of the Customer's Designated Tower Cluster to receive the Customer's Email on behalf of the Customer's domain on a 24x7 basis; and
- 3.2.2 In relation to the Customer's outbound Email it is the availability of the Customer's Designated Tower Cluster to accept the Customer's outbound Email from a correctly configured Customer SMTP host on behalf of the Customer's domain(s) on a 24x7 basis. Measurement of Email Service Availability will be via the Interoute tracker.
- 3.3 If in any calendar month Email Service Availability is below one hundred percent (100%) the Customer may be entitled to a percentage credit in accordance with the table below.

Percentage Email Service Availability per calendar month	Percentage credit of Monthly Charge
< 100% but > 99.0%	20
< 99.0% but > 98.0%	40
< 98.0% but > 97.0%	60
< 97.0% but > 96.0%	80
< 96.0% but > 95.0%	100
< 95%	Termination of Email Services at Customer's discretion

- 3.4 In the event that the Email Services are terminated such termination shall be the sole and exclusive remedy in contract, tort or otherwise with respect to Email Service Availability.

4. Latency

- 4.1 This Latency SLA will only operate if the Customer utilises one or more of the Email Services.
- 4.2 "Latency" means, as measured by the Interoute Tracker, the average round trip time for Emails sent every 5 minutes to and from every Tower. Times for the round trip of each Email are logged and used to produce a Latency report for each Tower for each calendar month. If the average roundtrip time of the Customer's Designated Tower Cluster exceeds the delays stated in the table below, the Customer may submit a Credit Request.

Average roundtrip time of < 95% of measurements (in minutes)	Percentage credit of Monthly Charge
> 2 but < 4	5
> 4 but < 6	10
> 6 but < 8	15
< 8 but < 10	20
> 10	25

schedule 2n

additional terms for MessageLabs services

- 4.3 This service level with regards to Latency will not operate during:
 - 4.3.1 Any Virus outbreak where the virus to Email ratio is greater than 1:200;
 - 4.3.2 Where a Customer causes a Denial of Service attack upon themselves or suffers such an attack from a third party;
 - 4.3.3 Delays caused by a mail loop from/to the Customer's systems.

5 Spam – False Positives

- 5.1 This False Positive SLA will only operate if the Customer utilises the Anti Spam Service.
- 5.2 Where the False Positive capture rate rises above 0.0004% of all Customer's Email traffic in any calendar month the Customer may be entitled to a credit in accordance with the table below.

Percentage False Positive capture rate during the calendar month	Percentage of Monthly Charge to be credited
>0.0004 but < 0.004	25%
> 0.004 but < 0.04	50%
>0.04 but < 0.4	75%
>0.4	100%

- 5.3 The following Emails will not constitute False Positive Emails for the purposes of this Clause 6:
 - 5.3.1 Emails which do not constitute legitimate business Email;
 - 5.3.2 Emails containing more than 20 recipients;
 - 5.3.3 Emails in which less than 80% of the Email content is in native English;
 - 5.3.4 Where the sender of the Email is on the Customer's blacklist;
 - 5.3.5 Emails which are sent from a compromised machine;
 - 5.3.6 Emails which are sent from a machine which is on a third party block-list;
 - 5.3.7 Emails which have been sent to more than 20 recipients and have at least 80% the same in content.
- 5.4 In order to be eligible for credit under this Clause, the suspected False Positive Emails must be sent to support@Interoute.com within two (2) days of receipt/time sent. Interoute will investigate and confirm whether or not the Email is a False Positive and will record the finding. At the end of the calendar month if the Customer believes the number of confirmed False Positives entitles it to a credit in accordance with the table above, the Customer must send a Credit Request to Interoute in accordance with Clause 2.1 of this Appendix.
- 5.5 The Customer recognises that investigation into suspected False Positive Emails in accordance with this Clause 0 incurs substantial administration by Interoute and its business Customers, therefore Interoute reserves the right to invoke, upon prior notice to the Customer, an administration charge of £100.00 per hour if in Interoute' reasonable opinion, the Customer is imposing an unacceptable administration burden on Interoute by requesting investigation into Emails which it is not reasonable to believe may constitute False Positives.

6. Spam – False Negatives

- 6.1 This False Negative SLA will only operate if the Customer utilises the Anti Spam Service.
- 6.2 Where the False Negative capture rate rises above 5% of all Customer's Email traffic in for the number of consecutive days stated below the Customer may be entitled to a credit in accordance with the table below.

Number of consecutive days during which the False Negative capture rate rises above 5% in any calendar month	Percentage of Monthly Charge to be credited
5	25%
10	50%
20	75%
21+	100%

- 6.3 This False Negative SLA will not operate where:
- 6.3.1 The Customer has not implemented Interoute' best practice for configuration;
- 6.3.2 The Email was not sent to a legitimate address;
- 6.4 In order to be eligible for credit under Clause suspected False Negative Emails must be sent to support@Interoute.com within two (2) days of receipt of the Email. Interoute will investigate and confirm whether or not the Email is a False Negative and will record the finding. At the end of the calendar month if the Customer believes the number of confirmed False Negatives entitles it to a credit in accordance with the table above, the Customer must send a Credit Request to Interoute in accordance with Clause 2 of this Appendix 2.
- 6.5 The Customer recognises that investigation into suspected False Negative Emails in accordance with this Clause incurs substantial administration by Interoute and its business Customers, therefore Interoute reserves the right to invoke, upon prior notice to the Customer, an administration charge of one hundred pound sterling (£100.00) per hour if in Interoute' reasonable opinion, the Customer is imposing an unacceptable administration burden on Interoute by requesting investigation into Emails which it is not reasonable to believe may constitute False Negatives.

7. Virus Infection

- 7.1 This non-infection SLA will only operate if the Customer utilises the Anti Virus Service. Ongoing research into Virus behaviour and anti-Virus technologies provides Interoute with an in depth perspective on the most effective anti-Virus strategies and software packages. As part of its managed service, Interoute is able to offer a 100% Service Level to protect the Customer's Customers from infection by 100% of all Viruses contained in Email which is capable of being scanned by AV. The Customer's systems are deemed to be infected if a Virus contained in an Email received through the Service has been activated within the Customer's systems either automatically or with manual intervention.
- 7.2 In the event that Interoute detects but does not stop a Virus-infected Email, Interoute will promptly notify the Customer, providing sufficient information to enable the Customer to identify and delete the Virus-infected Email. If such notification results in a prevention of infection the remedy set out in Clause 7.3 shall not apply. Failure of the Customer to promptly act on such information will invalidate this Service Level.
- 7.3 Should a Customer's systems be infected by one or more Virus in any calendar month during the Minimum Period as notified to Interoute by the Customer in a logged and validated support call confirming that a Virus has been passed to the Customer

schedule 2n

additional terms for MessageLabs services

through the Service, Interoute shall credit the Customer 100% of the Monthly Charge for the AV service or two thousand pounds sterling (£2000) whichever is the lower. The remedy set out in this Clause 7.3 shall be the sole and exclusive remedy in contract, tort or otherwise in respect of any infection of the Customer's systems by a Virus passed to the Customer through the Service. For the avoidance of doubt, the remedy set out in this Clause 7.3 shall not apply in cases of deliberate self-infection by the Customer.

8. Fault Response

8.1 Whenever the Customer raises a problem, fault or request for service information via telephone or Email with Interoute, its priority level is determined and it is responded to as defined in the table below.

Priority Level	Definition	Target
Critical	Loss of Service that cannot be circumvented	Acknowledged within 2 hours; Customer informed of progress at appropriate intervals.
Major	Loss of Service that can be circumvented, partial loss of Service or Service impairment	Acknowledged within 4 hours; Customer informed of progress at appropriate intervals.
Minor	Potentially Service affecting	Acknowledged within 8 hours; impact assessed and Customer informed of developments at appropriate intervals, if required.
Information	Non-Service affecting information request	Acknowledged within 24 hours; passed to appropriate owner within Interoute for due consideration and prioritizing according to assessed impact.

8.2 If the Customer believes that it has experienced a delay in Interoute's response to a request outside of the parameters defined above it may be entitled to a credit. **Credit Requests must state the time, date and the log number of the incident.** If eligible, the Customer will be credited in accordance with the table below.

Priority	Failure to meet target	Percentage Credit of Monthly Charge
Critical (up to a maximum of 5 incidents in any calendar month)	More than once in a calendar month	5
Major (up to a maximum of 6 incidents in any calendar month)	More than twice a calendar month	4
Minor (up to a maximum of 7 incidents in any calendar month)	More than three times in a calendar month	3
Information (up to a maximum of 20 incidents in any calendar month)	More than five times in a calendar month	2