

TECHNOLOGY WHITE PAPER

Anti-Spam

*Behind the scene of **Exclaimer Mail Utilities**' Anti-Spam solution*

Author: Gary Levell, Exclaimer Ltd
Ref: 300107



Exclaimer
UK +44 (0) 845 050 2300
USA 1-888-450-9631
info@exclaimer.com

Table of contents

Abstract	2
Introduction	2
How Anti-Spam works	4
How to deal with spam – the Exclaimer way.....	4
Too much junk in your Inbox.....	4
Unmanageable server queues.....	5
Bandwidth consumption	5
The tests in detail	7
Mission Critical Accounts	7
Manual Blacklist.....	7
Blocked IP	8
Spoofer IP.....	8
Spoofer Domain	8
Recipient not in the AD	9
Manual Whitelist.....	9
Trusted IP.....	10
SPF Fail.....	10
Auto Whitelist.....	10
SPF Softfail	11
DNS Whitelist	11
DNS Blacklist	12
DNS RHS Whitelist	12
DNS RHS Blacklist.....	12
Detection Center.....	13
SPF PASS	13
HTML Emails	14
Email with attachment.....	14
Unclassified	14
The actions in detail	16
Reject	16
Modify.....	17
Deliver	17
Other settings.....	18
The SPF Best Guess Policy	18
The 'Backdoor'	18
Conclusion	19
Glossary.....	20
Copyright Notice	23

▶ Abstract

This document covers:

- The problems caused by spam and what can be done to combat them.
- The various spam filtering features that Exclaimer Mail Utilities uses to identify and classify email.
- The actions that can be taken once an email has been classified and how this helps to maintain a manageable email system.

Being part of our core business we hope to shed some light on exactly what happens to your organization's email messages when they pass through our spam filter.

▶ Introduction

According to Commtouch® 87% of all email sent over the Internet in 2006 was spam. This was a 30% increase from approximately 107.7 billion spam messages per day in 2005 to 140 billion in 2006.¹

It's not just the amount of spam being sent over the Internet that has increased, but also the speed at which spammers are able to adapt to new filtering techniques. This has led to anti-spam developers creating more robust techniques in order to effectively separate the spam from the legitimate email messages.

Spammers use increasingly extravagant techniques to try to get their mail delivered. This has led to many anti-spam filters not being as effective as they once were, leading to calls to understand why spam is still being received and what can be done about it.

Our previous solution was based on the well founded principal of not (explicitly) checking message content, making us both language and format agnostic. This approach still works well but it has been improved.

The key has been to develop a series of reliable and robust processes that filter the spam as efficiently as possible. These can then be adapted and refined to combat the current levels and types of spam being sent over the Internet.

The latest incarnation of the Exclaimer Mail Utilities' Anti-Spam module utilizes some of the most up-to-date anti-spam filtering techniques to minimize the amount of spam you receive.

Our aim is to help you understand exactly what is being done to your email in order to show just how effective our system can be.

If you want to see the Exclaimer Mail Utilities Anti-Spam module in action simply download a 30 day trial version from <http://www.exclaimer.com/downloads>

¹ 2006 Spam Trends Report: Year of the Zombies, produced by Commtouch®, December 27, 2006

▶ **How Anti-Spam works**

The Exclaimer Mail Utilities Anti-Spam solution works in 2 phases.

Phase 1 - Classification

The message is subjected to scrutiny to determine if it is a spam message or not. This scrutiny does not just revolve around looking for characteristics that make it spam, it also looks for characteristics that might make it not spam (this is sometimes referred to as 'ham').

Phase 2 - Action

Once classified the message can be rejected, modified in some way (perhaps placing [SPAM] in the subject or redirecting it to a quarantine mailbox) or it can be delivered if the tests had determined that the message was a ham one.

▶ **How to deal with spam – the Exclaimer way**

The problems caused by spam broadly fall into these 3 categories:

1. **Too much junk in your inbox**
2. **Unmanageable Server queues**
3. **Bandwidth consumption**

Too much junk in your Inbox

Exclaimer Mail Utilities reduces this by being more aggressive with the bulk mail that was previously delivered to your inbox. If a message is classified by our detection centre as a bulk message, then it calls on several other more aggressive Domain Name Service Blacklists (DNSBL's) to help further classify the message.

These are:

- SpamCop
- NJABL
- SORBS

All of these services offer a variety of capabilities, but we have found that using all three of them permits an overlap which significantly reduces the incidents of spam in your inbox while maintaining our fiercely guarded false-positive ratio.

In conjunction with the more aggressive stance on these messages, Exclaimer Mail Utilities also provides both the ability to specify mission critical accounts which allow you to pick certain accounts for a reduced level of anti-spam checking. Exclaimer's new Auto-Whitelisting feature means you can whitelist people simply by sending them a message first.

You can even use Exclaimer's Auto-Whitelist wizard at the start of a new deployment of Exclaimer, all the people that your organization corresponds with are automatically added to the Whitelist. This allows for seamless integration into your current Exchange Server setup.

Unmanageable server queues

Many of the spam messages your organization receives are directed to non-existent email accounts, and it's not until you consider this carefully that you realize why this is happening.

Normally, this would result in an NDR being returned to the sender and it's this behavior that the spammer is trying to trigger.

After all, Non-Delivery Receipts (NDRs) and other Delivery Status Notifications (DSNs) are supposed to enjoy privileged behavior in the internet.

A sad side-effect of this is that, for the most part, the bounced recipient does not exist either (and in some cases neither does the domain), and this leads your Exchange server to get into a retry state which eventually leads into a message being placed in the badmail directory. This can fill up with so much junk that you can't even get Explorer to visit the directory to do anything about it.

In order to deal with this issue Exclaimer Mail Utilities only sends bounce messages to domains that result in an SPF pass. This means that the recipient is; a) likely to exist and, b) can do something about the backscatter if they didn't send the original message.

The net result is that Exclaimer Mail Utilities shows a significant reduction in the amount of undeliverable NDRs in your server queues.

Bandwidth consumption

On average a spam message is between 10 & 40K in size (a similar size to a single smallish image on a webpage). It is in the spammers' interests to keep their messages small as this allows them to send more messages to their "customers".

Many of our customers get between 500 – 2,500 spam messages per day. At 40K/spam message this is 100MB of bandwidth being consumed. If this is averaged out over the day it is about 1.1K/second. This is well within the bandwidth of current ADSL connections.

We have chosen to allow Exclaimer Mail Utilities to accept all messages in their entirety for complete analysis. This was primarily done to ensure that messages sent directly to your server were treated the same as those sent from secondary, backup or ISP mail servers.

It is possible to configure Exclaimer Mail Utilities to reject the message or connection as soon as possible to reduce bandwidth consumption. This can be done at the penalty of having to treat direct connections with spammers differently from spam that is relayed from another mail server under your control.

At Exclaimer HQ, we have to use our anti-spam software in this fashion.

▶ The tests in detail

Exclaimer Mail Utilities will classify a message as soon as it has all the data it needs to do so. Exclaimer usually defers processing of this classification until the entire message has been received (which in SMTP protocol terms, is after the DATA command has been completed).

Each test below indicates the point at which it can perform its classification. In all cases, the sequence of rules processed for action is the same, i.e. from top to bottom.

Exclaimer Mail Utilities does have a way to deal with the classification as soon as possible by clearing the "Defer anti spam checks until after DATA command" in the Advanced Settings dialog box.

Mission Critical Accounts

Mission critical accounts provide a way to bypass some or all of the other anti-spam tests for accounts that are more important than others. This might be 'sales@...' address if you are worried about false positives. These Mission Critical Accounts can be specified by AD account or SMTP address.

Obviously the reduced level of anti-spam checking means that these accounts will always seem to get more spam than ones that are not mission critical, although you can control exactly which future tests are pertinent to mission critical accounts.

The earliest point that this can be classified by Exclaimer is at the RCPT TO: phase.

Manual Blacklist

Manual blacklist provides a way to block messages based on combinations of details ranging from IP address through to envelope sender/recipient, message sender/recipients and even subject content.

This is a very powerful way to block messages that are not caught by other anti-spam tests. It can be used to help enforce compliance issues, such as preventing non-spammers from harassing employees.

The earliest point that this can be classified by Exclaimer depends upon the data that is present in the blacklist test.

If only IP address is specified, then this classification can happen at HELO/EHLO and then all other messages transmitted during this session will have at least this classification.

If Envelope FROM is specified then the earliest this classification can happen is at MAIL FROM:

If Envelope TO is specified then the earliest this classification can happen is at RCPT TO:

All other details require the message to be classified after the DATA command is complete.

Blocked IP

Blocked IP is similar to Manual Blacklist, but it offers the ability to block whole chunks of the internet. For instance, you might decide that you don't want to receive email from some particular ISP or country.

IP addresses are (loosely) broken up in to geographic units (at least at the larger levels), and within those, ISPs are allocated blocks of addresses.

It is possible to specify a range of addresses using the CIDR notation, e.g. 10.0.0.0/8 would be a range of 16777216 IP addresses from 10.0.0.0 thru 10.255.255.255.

The earliest point that Blocked IP can be classified is at HELO/EHLO.

Spoofed IP

Spoofed IP is when a sending mail server signs on in the HELO phase with an IP address as the HELO parameter that is not the same as its connection IP address.

Since this is such a trivial check to make, it's a wonder that this technique was ever used, but never the less, we still get 200 of these a day!

No legitimate email servers ever do this, and it's normally a virus Trojan trying to replicate itself to your system. This classification should always result in a rejected or quarantined message.

The earliest point that Spoofed IP can be classified is at HELO/EHLO.

Spoofed Domain

This classification is similar to Spoofed IP. This is where the sending mail server pretends that it's one of the domains that you are authoritative for in the HELO command.

It's a bit like someone ringing you and when you pick up the phone to answer and they say "Hello, it's George". Well, you know it's not George, because that's you. Daft huh?

We get 1500/day of this kind of attack.

The earliest point that Spoofed Domain can be checked is HELO/EHLO.

Recipient not in the AD

Recipient not in the AD is just as it sounds. It's a test designed to filter out messages to people who don't exist, and you'd be surprised at just how many of them there are. On an average day we receive 35,000 messages like this.

It is possible that this was just a mistyped email address. The sender will know this subject to some prerequisites, so you don't have to worry.

Obviously email classified as such would not normally constitute a problem for you since no one would ever see this email, but if your systems issue an NDR then some unsuspecting person may end up with a message telling them that they had sent a message that they hadn't.

There is a caveat to this test, which is if any of the recipients on the message are real, then this classification is not performed. For example, a message to a single person who is not in your AD will result in this test triggering as will a message to other non-existent people all of whom are not in the AD. If there is a single recipient who is in the AD, then this test will not trigger. Don't worry though, there are plenty of opportunities to catch this message if it is a spam one later.

The earliest point that Recipient not in AD can be checked is at RCPT:

Manual Whitelist

Manual Whitelist is similar in nature to the Manual Blacklist. You can use this to ensure that messages from certain sources, people or containing a certain combination of text characters in the subject are excluded from further anti-spam tests.

The earliest point that this can be classified by Exclaimer depends upon the data that is present in the Whitelist test.

If only IP address is specified, then this classification can happen at HELO/EHLO and then all other messages transmitted during this session will have at least this classification.

If Envelope FROM is specified then the earliest this classification can happen is at MAIL FROM:

If Envelope TO is specified then the earliest this classification can happen is at RCPT TO:

All other details require the message to be classified after the DATA command is complete.

Trusted IP

Trusted IP is a server that you know will never generate spam. This is usually a web server or other automatic system under your administrative control that can generate email messages.

You simply add the IP address (or subnet) of the machine that you are confident will never send spam.

The earliest point that this classification can occur is at HELO/EHLO.

SPF Fail

The SPF fail test is when the connecting mail server attempts to deliver messages from a particular domain and the SPF policy (stored in DNS) indicates that the connection mail server IP address is not acceptable.

SPF is intended to protect the domain and is checked by receiving mail servers. There are many systems on many different platforms that now check SPF policy and it is a great way to reject out-and-out spoofed domains and gives some credibility to those that pass.

Generally speaking mail servers that fail the SPF policy are subject to being rejected by many large ISPs and many mail server implementations.

The earliest point that this classification can be performed is at MAIL FROM:

Auto Whitelist

The Auto Whitelist is a list of smtp addresses generated by Exclaimer of all the recipients of outbound messages.

This means is that anyone you send email to will be able to reply without triggering most of the anti-spam tests. Obviously if they trigger any of the tests before this one, then they are subject to being classified differently.

Exclaimer comes with a wizard to enable a rapid setup of this file, and this will scan your entire Exchange organization extracting the smtp addresses of all the people you have sent email to or received email from. Deleted Items and Junk mail are obviously excluded from this scan.

Once this wizard has completed, Exclaimer will have a large database of all the people you regularly communicate with and this allows you to have a high degree of confidence that you won't miss an important email because of a misclassification.

There is a practical limit to the size that this list can become and we've defaulted this to 50,000 entries. Please make sure this is suitable for your needs prior to running the Auto Whitelist Wizard.

Old (stale) entries are removed in the natural course of time – correspondents that you communicate regularly with have their importance increased so that they are less likely to “fall off the end”.

The earliest point that this classification can be performed is at MAIL FROM:

SPF Softfail

This test is similar to SPF fail, but is not as aggressive. It merely indicates that the domain owner was unsure if the sending mail server was legitimate or not. The SPF specification states that this classification may be treated to more scrutiny.

You can chose to reject messages of this classification if you so wish.

Like the SPF Fail, the earliest point that this classification can be performed is MAIL FROM:

DNS Whitelist

DNS Whitelists are not as successful as once hoped, but there is good reason for an optimistic future. The theory is that if your IP address has a reputation for not sending spam, then you might be able to bypass irritating content based anti-spam systems.

This primarily targets large bulk mail senders and has so far not shown an ability to deal with legitimate mail list servers. This situation is sure to change over time which is the reasoning behind this classification.

The earliest point that this can be performed is at HELO/EHLO.

DNS Blacklist

If it weren't for DNS Blacklists email on the Internet would be simply impractical.

Exclaimer relies primarily on Spamhaus, who in our opinion operate one of the most professional services on the internet. We also refer to SpamCop, NJABL and SORB all of whom offer credible services albeit slightly more aggressive.

All of these organizations maintain lists of IP addresses that have sent or are currently in the process of sending spam. Some of them also maintain lists of dial-up address ranges and other machines that their subscribers would not like to communicate with.

Some of these DNS Blacklists are used to reject email from certain servers outright while others verify and classify email as bulk.

On our servers the DNS Blacklist classification currently traps about 55,000 messages/day.

The earliest point that this classification can be performed is at HELO/EHLO.

DNS RHS Whitelist

Where the DNS Whitelist classification is attempting to check the IP address of the incoming mail server, the RHS variation checks the domain of the sender for his reputation.

Again, there is very little available in this category at the present.

The earliest point that that this classification can be performed is at MAIL FROM:

DNS RHS Blacklist

DNS RHS Blacklists only provide a way to trap a small amount of spam. The service provider that we use is bogusmx at <http://www.rfc-ignorant.org/>. This is a list of domains that have been proven to use bogus MX records.

This was once a way for a spammer to bypass naïve checks that the sending domain had an MX record in DNS without actually having to have a mail server.

The earliest point that this classification can be performed is at MAIL FROM:

Detection Center

The Detection Center monitors spam outbreaks and trends, and classifies the messages accordingly. In order to reach their target audience spammers have to operate campaigns with hundreds of millions of messages. This kind of activity has a consequence especially when looking at patterns of email traffic over the world. You can observe our real time monitor on the website www.exclaimer.com/antispamoutbreakmonitor.aspx and see outbreaks happening in real-time.

The Detection Center will classify messages as Spam, Bulk or Not Spam. We further sub-classify the Bulk messages by also referring back to the more aggressive DNS Blacklists and we also check the sending domain to see if it passes the domain SPF policy.

The earliest point that these classifications can be performed is after the DATA command is complete.

Detection Center – Bulk (SPF_PASS)

Messages that are confirmed bulk (and are not sent from servers that appear in the more aggressive DNS Blacklists) where the domain sending them has an SPF policy that results in a PASS will have this classification.

This is normally a 'white' classification since the sender has had to go to considerable effort to get this message delivered. For example, being checked against no less than 4 public anti-spam list providers and being classified as a bulk email sender.

Detection Center – Bulk

Bulk messages are still checked with the more aggressive DNS Blacklists which (if needed) will override the bulk classification.

Detection Center – Spam

The message is part of an ongoing spam outbreak.

SPF PASS

Messages that result in an SPF pass will be classified with this test. This allows for a very aggressive stance to be taken, for example, you can choose not to accept unsolicited messages from domains that do not result in an SPF pass.

This kind of aggressive stance on email messages should only be taken with the full knowledge that you will only receive messages that are sent from servers that result in an SPF PASS.

However, this test does not guarantee that a message is not spam, it merely ensures that there is a high degree of probability that the sender of this message is; a) genuine,

b) sent the message and, c) can deal with the spam problem if that is what it is.

The earliest point that this classification can be performed is at MAIL FROM:

HTML Emails

Exclaimer does not have a scenario that uses this classification; however, it can be useful for very aggressive mail administrators who do not want to permit HTML email unless the sender is white listed.

This may seem quite tough but it can deal with a large portion of spam that comes in this form.

The earliest point that this classification can be performed is after the DATA phase.

Email with attachment

Exclaimer does not have a scenario that uses this classification; it can be useful for very aggressive mail administrators who do not want to permit email that has attachments unless the sender is white listed.

This may seem quite tough, but it can deal with a large portion of spam that comes in this form.

The earliest point that this classification can be performed is after the DATA phase.

Unclassified

Messages that have remained unclassified through all the previous white and black testing will have this classification.

This classification could be used to implement a 'challenge-response' type solution.

Challenge-Response on its own is generally regarded as a bad technique to combat spam. Nevertheless, it is a very effective solution and this is what initially attracts people to it. This kind of approach is generally considered bad practice because the backscatter generated from challenging every spam message simply adds to the problem on the internet rather than reducing it.

However, if you choose to implement a challenge-response approach then we recommend you use as many of the previous tests to classify the message in other ways before issuing a challenge.

This is the premise behind the 'Hardened' scenario where messages that are not classified as spam or ham that do not result in SPF pass are issued a challenge.

▶ The actions in detail

The actions are how Exclaimer deals with messages that are classified by particular tests. There are three ways to deal with these classifications:

1. **Reject the message**
2. **Modify the message**
3. **Deliver the message**

Reject

When rejecting a message it is polite to include a reason why. Unfortunately this will not affect or inconvenience a spammer in any way - they cannot realistically take any notice of it. However, for misclassified senders this can help diagnose why their messages are not being delivered.

Exclaimer behaves differently depending upon when the action is taken. Although most of the time it only processes messages at the end-of-DATA.

Rejection at HELO

Exclaimer will not reject any messages at the HELO phase. Doing so would result in a violation of RFC2822 and this would lead to incorrect behavior for legitimate mail servers that were incorrectly classified. There is little detriment to deferring this until the next phase, although any classifications that have been established will persist for the session.

Rejection at MAIL FROM

The connection mail server will receive a rejection response. This normally is in the form '550 Spam not accepted' and directs a legitimate mail server to issue an NDR to the sender.

Rejection at RCPT TO

Exclaimer does no action at RCPT TO to allow all the recipients of the message to be specified (and classified) before taking action.

Rejection at start of DATA

The connection mail server will receive a rejection response. This normally is in the form '550 Spam not accepted' and directs a legitimate mail server to issue an NDR to the sender.

Rejection at end of DATA

If the domain in the MAIL FROM command of the connecting mail server did not result in an SPF pass then the connection mail server will receive a rejection

response. This normally is in the form '550 Spam not accepted' and directs a legitimate mail server to issue an NDR to the sender.

If the domain resulted in an SPF pass, a bounce message will be generated. This allows a higher fidelity message (with better chance of being read and acted upon). This message will indicate why the original message was not delivered and what (if anything) can be done about it.

Modify

Messages can be modified in any of the following ways:

- Spam Confidence Level can be set (Affects Exchange 2003/Outlook 2003 native systems only)
- An internet header field can be modified
- The Subject can be modified
- The messages can be redirected to another account (perhaps a Quarantine mailbox).

You can choose to continue processing other anti-spam rules after this action has been taken or not.

Deliver

No further anti-spam tests will be applied to this message. It will be delivered without being modified (apart from some useful internet headers which can be used to diagnose problems).

▶ Other settings

The SPF Best Guess Policy

Many large domains such as gmail.com already publish their SPF policy in DNS, which provides a fabulous way to prove (or disprove) that an email is legitimately from that domain.

However, many smaller domains do not have a policy and because of that it's not possible to use the SPF classification to help the war on anti-spam.

Exclaimer provides a 'best guess' policy that seems to fit most other domains. It is used to test for SPF_PASS, and not to indicate an SPF_FAIL.

This policy simply says that if the message is received from an IP address in the /24 net block of your MX server or an A record in DNS, then this will presume to be an SPF pass.

The 'Backdoor'

Many of the anti-spam tests come after the Manual Whitelist test, and this can be used to create a 'backdoor' so that blocked senders can self-help and get a critical message through without having to contact you using alternative methods.

If the backdoor code is present then bounce messages generated in the Reject action will contain a paragraph indicating how the sender can bypass the anti-spam checks and get a message through.

▶ Conclusion

When dealing with the ever changing and dynamic environment of Anti-Spam it is important that whatever system you decide to use maximizes results whilst minimizing setup and maintenance costs.

As an Anti-Spam provider we always aim to keep the number of updates that customers have to apply to their mail servers to a minimum. Given the increase in spam attacks over the last few months we hope that with the changes we have made to Exclaimer you can enjoy a reasonable period without having to make any major updates.

Our aim is to give you an Anti-Spam solution that provides you with a robust and reliable upgrade to your existing Mail Utilities Anti-Spam module.

But don't just take our word for it – Why not try it for yourself?

Download your free 30 day trial version of Exclaimer Mail Utilities (including Anti-Spam and Anti-Virus) at <http://www.exclaimer.com/downloads>.

If you have any questions or want to find out more about any of our products please call Sales on (UK) **+44 (0) 845 505 2300** or (US) **1-888-450-9631**. Alternatively, you can email sales@exclaimer.com.

▶ Glossary

Blacklist

A list of email addresses or IP addresses that individuals and organizations can use to filter out unwanted emails.

DNS

Domain Name Service - used on Internet for translating hostnames into Internet addresses. For example, <http://www.exclaimer.com>

EHLO

Extended HELLO – used to open a transmission with ESMTP clients.

FQDN

Fully Qualified Domain Name – an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. For example, 'somehost.example.com'.

HELO

HELLO - used to open a transmission with ESMTP clients.

HTML

HyperText Markup Language – used predominantly for web page creation.

HTTP

HyperText Transfer Protocol – used to transfer information on the World Wide Web.

IP Address

Internet Protocol - a unique number that devices use to identify and communicate with each other on a computer network.

ISA server

Microsoft Internet Security and Acceleration Server – a firewall or proxy server which runs on Windows 2000 and Windows Server 2003.

ISP

Internet Service Provider - a business or organization that provides access to the Internet and other Internet related services.

MTA

Mail Transfer Agent – a Mail Server or Mail Exchange Server.

MX

Mail Exchange record - a type of resource record of the Domain Name Service (DNS) specifying where Internet email should be routed.

NDR

Non-Delivery Report - a message that tells the sender that their message could not be delivered.

PRA

Purported Responsible Address - usually the From: address, but can be other pieces of information in certain circumstances.

PTR

Pointer Record – used to map an IPv4 address to the canonical name for that host.

RFC 1918

A published paper that specifies Internet Best Current Practices for the Internet Community.

RFC 281

A published paper suggesting an addition to File Transfer Protocol.

RFC 2821

A published paper that specifies Internet standards track protocol for the Internet community.

RFC 2822

A published paper that specifies a syntax for text messages that are sent between computer users, within the framework of email messages.

RHS list

Right Hand Side – a list of email address domains.

SMTP

Simple Mail Transfer Protocol – used as the standard protocol for email transmissions across the Internet.

SPF

Shortest Path First - a routing method able to eliminate loops. Also, Sender Policy Framework - an extension to the Simple Mail Transfer Protocol (SMTP), SPF allows software to identify and reject forged email addresses in the SMTP MAIL FROM (Return-Path).

TCP/IP

Transmission Control Protocol/Internet Protocol – also known as the Internet protocol suite. A set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run.

Trojan machine

A computer that has been infected and taken over by a Trojan computer virus. Often used by spammers to send unsolicited email.

Whitelist

A list of email addresses or IP addresses that individuals and organizations use to identify senders they wish to receive email from.

▶ Copyright Notice

The information in this document is subject to change without notice. Exclaimer Ltd assumes no responsibility for any errors that may appear in this document. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious and not associated with any real company, organization, product, domain name, e-mail address, logo, person, place or event.

Exclaimer Mail Utilities and other Exclaimer devices are either registered trademarks or trademarks of Exclaimer Ltd in the United Kingdom and/or other countries. Exclaimer may have trademarks, copyrights or other intellectual property rights covering subject matter in this document. All other company and product names are acknowledged as being the trademarks or registered trademarks of their respective companies.

Unless expressly provided in a written license agreement from Exclaimer Ltd, the furnishing of this document does not give you any license to these trademarks, copyrights or other intellectual property.

Copyright 2007, Exclaimer Ltd. All rights reserved. This document may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without the express written permission of Exclaimer Ltd. Complying with all applicable copyright laws is the responsibility of the user.