

# Complying with New Zealand's Anti-Spam Legislation

Updated August 2009

## INTRODUCTION

The New Zealand Government has recently passed legislation outlawing the transmission of unsolicited commercial messages. Starting on September 5, 2007 the Unsolicited Electronic Messages Act comes into force. After this date, heavy penalties can be levied against individuals or companies found to be breaching the Act.

The Act doesn't just apply to spammers, however. Organizations are forbidden to send commercial messages without the express consent of the recipient, which must be granted prior to the first message being sent. A commercial message is defined within the Act as an electronic message that markets or promotes goods, services, land, or investment opportunities. Normal business communications between companies and individuals are not included in the commercial email terminology as defined by the Act.

Additionally, all commercial messages are expected to include functional unsubscribe facilities, which must be presented in a clear and conspicuous manner within the body of the message.

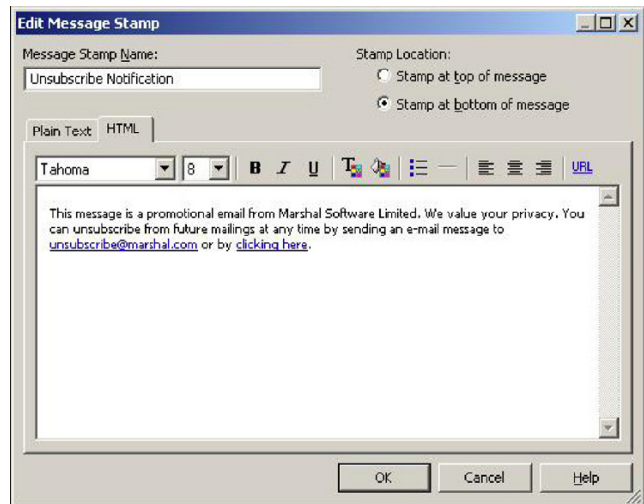
MailMarshal SMTP can be used to help organizations comply with the Act by ensuring that their marketing materials are not inadvertently delivered to recipients who have not yet given consent, or who have expressly declined to receive future commercial communications.

## HOW CAN M86 SECURITY HELP?

M86 Security offers a number of features which it believes can assist you to comply with the Unsolicited Electronic Messages Act 2007. M86 has set out technical assistance in respect of these products below.

## STAMPING UNSUBSCRIBE INSTRUCTIONS

Leveraging MailMarshal SMTP's message stamping feature is a simple way to ensure that outgoing commercial emails always contain an unsubscribe facility. To do this, administrators should create a message stamp from within the MailMarshal Configurator similar to following:



In our example, the [unsubscribe@yourdomainhere.zz](mailto:unsubscribe@yourdomainhere.zz) email address is a mailto: link that generates a new message addressed to [unsubscribe@yourdomainhere.zz](mailto:unsubscribe@yourdomainhere.zz) with the word 'Unsubscribe' in the subject line. The following HTML markup was used:

```
<a href="mailto:unsubscribe@yourdomainhere.zz?Subject=Unsubscribe">unsubscribe@yourdomainhere.zz</a>
```

In addition, we've included a link to our Web mailing list unsubscribe facility; by clicking on the link, the user will instantly be unsubscribed from future mailings. Our link includes the recipient's email address as a parameter to a CGI script running on our web server. The following HTML markup was used:

```
<a href="http://www.yourdomainhere.zz/marketing/unsub.cgi?address={Recipient}">clicking here</a>
```

Notice that a MailMarshal variable, "{Recipient}", was used within the link. If a message addressed to [ceo@whizbang.zz](mailto:ceo@whizbang.zz) was stamped with this message, the link that would be stamped into the message would be:

```
http://www.yourdomainhere.zz/marketing/unsub.cgi?address=ceo@whizbang.zz
```

There is an important limitation to using the {Recipient} variable to populate a URL query string – messages must be addressed to only one recipient. Messages with multiple recipients will have the full recipient list within the query string, potentially causing a single unsubscribe request to unsubscribe an entire mailing list.

Now that the message stamp has been created, it is a simple matter to utilise it to stamp outgoing marketing messages. Administrators might create a rule like the following:

**Standard Rule: Add Unsubscribe Notification to Marketing Emails**  
*This rule adds a block of text to the end of marketing messages containing instructions on the availability of our unsubscribe facilities.*  
When a message arrives  
Where message is outgoing  
Where addressed from '[Marketing and Promotional Addresses](#)'  
Stamp message with '[Unsubscribe Notification](#)'  
And pass message to the next rule for processing.

## PROCESSING AND ENFORCING UNSUBSCRIBE REQUESTS

MailMarshal SMTP's dynamic groups can be utilised to maintain a list of individuals who have opted out of marketing communications from an organisation. In addition, these groups can be used to prevent marketing messages inadvertently being sent to disinterested parties, protecting the company from potential legal liability and embarrassment.

First, a rule should be created to add users to the unsubscribe list who have emailed the published unsubscribe email address. This rule should look like the one below:

**Standard Rule: Process Unsubscribe Requests**  
*This rule adds email addresses to the 'Unsubscribe Requests' group if the remote sender has emailed the unsubscribe address.*  
When a message arrives  
Where message is incoming  
Where addressed to '[unsubscribe@yourdomainhere.com](mailto:unsubscribe@yourdomainhere.com)'  
Move the message to '[Unsubscribe Requests](#)'  
And add message sender into '[Unsubscribed Addresses](#)'

To ensure that promotional messages aren't inadvertently delivered to individuals who have opted out of future communication, a rule could be created to block outbound marketing messages to those addresses. We've chosen to send a message to the mailing list administrator, informing them of a potential issue. It would also be possible to set up message digests on the 'Mailing List Corrections' folder to notify an administrator periodically. The rule should look like the one below:

**Standard Rule: Block Marketing Message to Unsubscribed Addresses** When a Message Arrives  
Where message is outgoing  
Where addressed both to '[Unsubscribed Addresses](#)' and from '[Marketing and Promotional Addresses](#)'  
Send a '[Policy Risk out](#)' notification message  
And move the message to '[Mailing List Corrections](#)'

## ENSURING YOU HAVE CONSENT

MailMarshal can import lists of email addresses from several sources, and use those addresses to ensure that marketing materials are not inadvertently sent to users who have not consented to receiving the materials.

Lists of addresses can be entered by hand into MailMarshal, imported from text files, or retrieved from LDAP servers housing mailing lists.

In addition, it is possible to use custom external commands to determine group membership from mailing list database servers.

Once the group has been imported, preventing erroneously-addressed marketing materials from leaving an organisation is as simple as creating a rule similar to the one below:

**Standard Rule: Block Marketing Material to Unknown Addresses**  
*This rule blocks marketing messages to email addresses not on our opt-in list and sends an alert to the mailing list administrator.*  
When a message arrives  
Where message is outgoing  
Where addressed from '[Marketing and Promotional Addresses](#)'  
Except where addressed to '[Opt-in List](#)'  
Send a '[Policy Risk out](#)' notification message  
And move the message to '[Mailing List Corrections](#)'

## ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit [www.m86security.com](http://www.m86security.com).

DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, M86 SECURITY PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of M86 Security, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Marshal. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data. This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. M86 Security may make improvements in or changes to the software described in this document at any time.

© 2009 M86 Security, all rights reserved.

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the U.S. Government is subject to the terms of the M86 Security standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Marshal, MailMarshal, the M86 Security logo, WebMarshal, Security Reporting Center and Firewall Suite are trademarks or registered trademarks of M86 Security or its subsidiaries in the United Kingdom and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

## TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



**Corporate Headquarters**  
828 West Taft Avenue  
Orange, CA 92865  
United States

Phone: +1 (714) 282-6111  
Fax: +1 (714) 282-6116

**International Headquarters**  
Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom

Phone: +44 (0) 1256 848080  
Fax: +44 (0) 1256 848060

**Asia-Pacific**  
Suite 1, Level 1, Building C  
Millennium Centre  
600 Great South Road  
Auckland, New Zealand  
Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 09.01.09