



Messaging Anti-Abuse Working Group (MAAWG) Vetting Best Common Practices (BCP)

November 2011

Introduction..... 1

Why Vet?..... 2

Pre-Send Vetting Techniques..... 2

Corporate Entity Formation and History 2

Infrastructure and Process 2

Sending History and Patterns 3

List, Data Collection and Management Practices..... 5

Post-Send Vetting Techniques 6

Methodology 6

Tools and Resources 7

WHOIS 7

Additional resources and tools for vetting the corporate entity 8

Introduction

Email Service Providers (ESPs), who send large volumes of email on behalf of their clients, are at the mercy of their worst clients' worst practices. Common problems such as e-appending, poorly run affiliate programs and past data corruption can create delivery and reputational issues not only for an ESP's problem senders, but for all of the ESP's other clients as well.

The Messaging Anti-Abuse Working Group (MAAWG) membership includes a variety of ESPs who have come together for healthy conversations about how to vet clients to avoid these issues. After much discussion, it became evident that not all ESPs use the same methods. This document is intended to summarize the various techniques in use and present them here as a resource for all ESPs. Not all techniques will be valid for all types and sizes of ESPs or their clients.

This document is intended as a resource for providers who are building and maintaining a client-vetting program for reviewing prospective and existing customers. It covers the general intent, purpose and benefits of a vetting program; specific guidelines on the process; the operation and criteria for vetting customers before they mail; and monitoring after the initial send.

This document is a broad “how-it’s-done” guide to vetting methodology. It is intended as a general guideline. Parts of the document will be useful for specific internal departments such as sales, compliance or other areas involved in client vetting. The document includes several different types of vetting techniques. This document is not intended to give guidance on specific vetting metrics (for example, what complaint rate thresholds to maintain).



Messaging Anti-Abuse Working Group

P.O. Box 29920 ■ San Francisco, CA 94129-0920 ■ www.MAAWG.org ■ info@MAAWG.org

Why Vet?

ESPs take on significant risk every time a new customer sends email. A bad client can undermine the sending reputation for the ESP's other clients as well as inflict abuse at recipient domains. When proper pre-send vetting is performed, ESPs can preempt damage caused by bad clients to both recipient domains and to their own sending reputation. With the effective post-send vetting techniques outlined below, bad clients who have successfully completed the initial assessment can also be discovered after they mail.

Vetting can also be a powerful tool for building sustainable clients and improving long-term client relationships. Many times, in-depth analysis of how prospective clients build and maintain their lists of email recipients will reveal issues that the client can correct. The vetting process provides the ESP with a unique opportunity to advise both prospective and existing clients on best practices and compliance.

Pre-Send Vetting Techniques

Below are several sets of questions customer-facing staff can use to establish whether a prospective customer qualifies for service.

Corporate Entity Formation and History

1. What is the name and address of the company?
2. How long has the company operated?
3. Does the company operate under any additional names or locations or has it done so in the past?
4. Who are the principals of the company?
5. Who will be our primary point of contact?

A review of public information about the company, its formation, and the business activities of its principals may be useful in establishing the *bona fides* of a prospective sender. Commercial entities are generally required to file information with their local taxation authority. This includes filing articles of formation, obtaining a business license, or filing notification of an assumed public alias (known as a "DBA") with the authority. In the United States, this is generally the Department of State for the state in which the company was formed. Most Departments of State provide free online access to some or all of these filings, as they are matters of public record.

An absence of filings may indicate a problem sender, particularly if the prospective customer otherwise indicates a long business history. Additionally, a business with a very short history or with principals who seem to form and disband multiple entities within a relatively short period may warrant additional scrutiny. Refer to the Tools and Resources section of this document for sources of free or low-cost corporate entity information.

Infrastructure and Process

1. Have you worked with an ESP(s) before? If so, which ESP(s) and what was your reason for leaving?

Prospects may have worked with multiple ESPs in the past or state they have left other service providers for deliverability reasons. These responses generally should be treated as red flags. It is important to discover and understand the essential reasons why your prospect is switching ESPs.

2. Do you know the IP address(es) you used for previous email marketing? If so, please provide the previous IP address(es).

There are many factors that affect ISPs' decisions to place email in the inbox or the spam folder. One factor is the reputation associated with the IP address from which mail originates. An IP address is a unique, static network identifier for computers and servers. In large part, ISPs determine how to handle mail based on the quality of the reputation associated with its originating IP address. ISPs measure reputation using data acquired from third parties, from historical data they maintain internally, or some combination of these. If the IP addresses previously associated with a potential client have been blocked or otherwise tainted, it could indicate a potential problem that needs to be further investigated and clarified.

3. Which domain(s) do you own and use in conjunction with your email marketing program? How long have you owned them? Is your domain registered using anonymizing information?

A common tactic of abusive senders is to hide their identity behind an anonymized domain registration. Legitimate senders have no need to hide corporate contact information when sending permission-based email. See the Tools and Resources section of this document for more information in the WHOIS discussion.

4. Do you monitor role accounts (e.g., postmaster@, abuse@)? If so, who manages this activity?

Whatever the quality of recipient lists and senders' practices, senders should expect complaints from recipients. Recipients frequently forward complaints via email to abuse@ or postmaster@ addresses for the sending domain. It is an industry best practice¹ to maintain and monitor mailboxes for each of these role addresses.

5. Do you have control over your DNS record? Does it make use of any authentication protocols?

The Domain Name System (DNS) provides a means for domain name owners to store other types of data that are essential for each domain's various data-handling functions. If senders are able to access and edit the DNS record for their sending domain(s), they can publish authentication records to assure recipient domains that the ESP is authorized¹ to send on their behalf.

Sending History and Patterns

1. What types of email messages do you send and in what proportions? Can you provide samples of the different types of messages you have sent or plan to send?

Examples include promotional and marketing, transactional and order confirmations, alerts, sales team outreach, event invitations, and other types of messages. Promotional and marketing messages typically suffer higher complaint rates and delivery issues than other types, even assuming a similar level of permission for all. Accurate answers to this question can give the ESP some level of expectation regarding frequency and magnitude of delivery issues.

¹ [RFC 2142 MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS.](#)

2. Do you segment your lists or do you send messages to all of your contacts each time you mail? If you segment, please describe the criteria used to segment.

Generally speaking, campaigns sent to segmented, targeted lists tend to perform better in most respects than campaigns sent to a large generic list of addresses subscribed from different places. Accurate answers to this question can give the ESP some level of expectation regarding frequency and magnitude of reputation (and concomitant delivery) issues.

3. How often do you mail to your lists and when was the last send?

Best email marketing results are attained by sending timely, relevant and expected email to subscribers. Senders that set and meet appropriate expectations with regard to content and frequency generally produce fewer delivery issues.

4. Do you share your list with anyone, including partners, advertisers or other brands in your own company? Do you send messages to your list on behalf of partners or third parties? If so, do you disclose to recipients at the time of collection that their addresses may be shared? How is this disclosure made?

Unexpected email from third parties or brands will generate complaints, even from otherwise strongly permission-based recipients. Accurate answers to these questions can give the ESP some level of expectation regarding frequency and magnitude of complaint issues.

5. Do you engage in affiliate marketing? If so, do you operate your own affiliate program or is it managed by a third party (e.g., Commission Junction or other vendors)?

Mail from affiliate marketers, or senders who mail on behalf of other entities typically in exchange for a commission, bears an additional degree of scrutiny. While many affiliate programs succeed by only sending to permission-based lists, affiliate programs as a broad category have historically been a vector for abuse. Programs operated by well-known, reputable third parties are typically less problematic than the do-it-yourself variety.

6. Has your domain or IP address ever appeared on a block list? What was the reason given for the listing and how did you address the issue?

DNS and domain-based block lists publish assertions about the historical quality of mail associated with IP addresses or domains. These assertions are frequently used by recipient domains as a source of reputational data to help decide how inbound mail from those sources will be handled. Possible constructive responses to a block listing generally include a review of list acquisition or hygiene procedures and implementation or tightening of sender best practices. Any answer that hints at infrastructure changes to evade a block listing is a potential red flag.

7. Do you have any data or metrics you can provide for messages sent over the last 3 months (e.g., deliverability, complaints, etc.)?

Measurements of prospective senders' historical performance can give some insight into the general quality of their lists and are therefore a useful indicator of the likely frequency or magnitude of potential issues. Poor historical performance, for example, may indicate deficiencies in the manner in which the senders' lists are assembled and maintained. In these instances, additional scrutiny may be appropriate.

List, Data Collection and Management Practices

1. How do recipients opt-in to your lists? Please list the points of contact and address collection, including online and off-line sources. For each point of collection, please include how consent or notification of future messaging is conveyed.

Senders should create and maintain an auditable trail that sufficiently demonstrates the method, date and source of permission for each intended recipient or group of recipients.

2. Were you or your previous ESP signed up to receive FBL (Feedback Loop) complaints? If so, what action did you take on complaints received?

Feedback loop complaints are automatically generated notifications made by many recipient domains to senders of mail, and arise when a recipient marks a message as spam, usually with a specific button within the email client. The ISP forwards this information to the sender or their ESP. The industry best practice is to unsubscribe recipients who report mail as junk and investigate to remedy the root cause.

In some instances, the complaint may be the result of a poor implementation of permission-gathering practices. If permission for the recipient is inadequate, the response to this question should indicate that a review was undertaken of how permission was collected for the recipient reporting the message as spam and of other recipients for whom permission was collected using the same or a similar methodology. It may also include an attempt to reconfirm those recipients.

In other instances, the spam complaint may be, essentially, a malformed unsubscribe request. If permission for the complaining recipient is strong, a response to this question from the sender should consider that subscriber expectations of content or frequency were not sufficiently met.

3. How did you manage unsubscribe requests? Have you taken steps to remove unsubscribed addresses from the list you have provided to us?

Removing unsubscribed addresses is not only a best practice, but is a legal requirement in the United States, Canada and the European Union. Be sure that suppression lists, or lists of recipient addresses that have been unsubscribed, are used and maintained and can be ported to new or additional sending platforms.

4. How did you previously manage bounces? Did you treat hard (5xx) and soft (4xx) bounces differently?

It is a best practice to remove addresses that generate hard bounces (alternately referred to as NDRs or 5xx bounce types) multiple times within a given period. There may have been automated policies in place at the sender's previous ESP to suppress these addresses.

While 4xx bounces (alternately referred to as soft bounces) are not indicative of any recipient-level condition, recurring high generic soft bounce rates may be indicative of content or sender reputation problems. An appropriate response to the question might include a resolution of persistent soft-bouncing issues.

5. Have you ever purchased a list? Do you rent lists or participate in affiliate marketing or co-registration? If so, provide details.

Affirmative answers to these questions should be a red flag. Purchased lists typically are comprised of addresses of recipients who have never consented to the email. Many ESPs will not allow senders to use purchased lists. The ESP should review all customer-supplied lists for any indication that they might be purchased (e.g., list headers that include terms such as “jigsaw,” “append,” etc.).

While co-registration lists might be accurately described as permission-based, the permission is usually of an uninformed variety. These lists therefore tend to perform as poorly as purchased lists.

6. Does your list contain common distribution and role accounts (e.g., sales@, staff@, support@)? May we review your lists prior to your provisioning?

Distribution and role accounts are typically never used for opting into a mail list and their appearance on a customer list may be indicative of poor acquisition practices, including list purchase. The ESP should review any customer-supplied lists for the presence of common role accounts or other known trap addresses.

7. Do you have a published privacy policy on your website?

The absence of any published privacy policy is another red flag. ESPs should review the content of the sender’s published privacy policy to ensure it does not appear to contradict any of the practices the sender describes in answers to this questionnaire.

Post-Send Vetting Techniques

This section describes techniques for vetting potential senders through completion of a limited test send. It also includes ongoing vetting once the sender has been provisioned in a production environment.

Methodology

Following satisfactory completion of the pre-send vetting, ESPs may allow the sender to complete a test send of messages to a small, randomly selected segment of their lists. The objective of the test is to gather key metrics about the mail stream that might give an early indication of potential problems in advance of provisioning the sender in an unfettered production environment.

The recommended size of the test can vary depending on the size of the client’s overall lists. However, test sends to fewer than ten thousand recipients may not yield statistically significant results.

Key metrics to review following the test send are largely typical of the metrics ESPs would monitor for existing customers. These might include:

- Overall bounce rate
- Relative percentage of various bounce types
- Open and click-through rates
- Unsubscribe rate
- Direct complaints
- Opt-out comments
- Spam complaint rate
- Complaint rate by domain or FBL

Any metric that varies significantly from other, existing senders of similar mail bears additional scrutiny.

Once the client has been vetted and provisioned, best practices for ongoing vetting include the continuous monitoring of these same metrics, as well as close monitoring of the following conditions:

- Significant and sudden increases in list size
- Content changes following significant changes in metrics
- Changes in the sender's published privacy policy following significant changes in metrics or volume
- Frequent changes of customer contact or payment information
- Stops and starts in activity that might indicate attempts to dilute poor reputation metrics over more than one ESP

Tools and Resources

This section serves as a guide for tools and resources that can be used in sender vetting and auditing.

WHOIS

WHOIS is a query and response protocol used to publish and access registration information of Internet resources.² During the vetting process, ESPs can take advantage of this tool to verify if a particular sender is representing their domain name correctly and whether there is transparency of information, should a particular domain name come under question. It is a MAAWG sender best practice that a customer reflect verifiable information when representing domain ownership and the information should not be obfuscated or hidden under a privacy tag with a postal box. WHOIS can also be used to verify contact information for a company's abuse help desk.

Example of a good registration practice verified by WHOIS:

```
mycomputer:~ user$ whois example.com
```

Registrant:

Inc, example.com

example.com,Inc

14 Circle Road.

Circle City, CA 90004

US

Domain Name: EXAMPLE.COM

Administrative Contact:

Inc, Example.com info@example.com

Example.com,Inc

14 Circle Rd.

Circle City, CA 90004

US

650-555-5555

Technical Contact:

DNS Admin dnsadmin@example.com

Example.com,Inc

14 Circle Rd.

Circle City, CA 90004

US

650-555-5555

² <http://en.wikipedia.org/wiki/Whois>

Example of bad registration practice verified by WHOIS:

mycomputer:~ user\$ whois example.com

Registrant:

I am a Proxy, Inc.

iamaproxy.proxy

P.O. Box 1111

Proxy City, Proxy State 88888

United States

Domain Name: EXAMPLE.COM

Administrative Contact:

Private, Registration EXAMPLE.COM@iamaproxy.proxy

I am a Proxy, Inc.

iamaproxy.proxy

P.O. Box 1111

Proxy City, Proxy State 88888

United States

(555) 555-5555 Fax -- (555) 555-5555

Technical Contact:

Private, Registration EXAMPLE.COM@iamaproxy.proxy

I am a Proxy, Inc.

iamaproxy.proxy

P.O. Box 1111

Proxy City, Proxy State 88888

United States

(555) 555-5555 Fax -- (555) 555-5555

Additional resources and tools for vetting the corporate entity

These include:

- Dun & Bradstreet (<http://www.dnb.com/>)
Provides business information
- LexisNexis (<http://www.lexisnexis.com/risk/>)
The Risk Solutions division provides financial and background information
- The Better Business Bureau (<http://www.bbb.org/online/>)
List complaints against a business
- PACER (<http://www.pacer.gov/>)
Provides online access to U.S. Appellate, District and Bankruptcy court records and documents nationwide; helpful to determine if the entity or principal was party to any email related legal action
- MAAWG [Senders Best Communications Practices, Version 2.0a, updated July 2011](#)
Defines best practices for sending email by high-volume email senders.