Thindata 1-1
A TRANSCONTINENTAL COMPANY

The Marketer's Guide to Successful Email Delivery

Part One | Best Practices

Spring, 2010

Inside This Document

PUBLISHED BY

Thindata 1:1
Inquiries@thindata.com
www.thindata.com

90 Eglinton Avenue East, 3rd Floor, Toronto, Ontario, M4P 2Y3, Canada
Toll Free: 1-866-361-3522

1152 West 2240 South, Suite B, Salt Lake City, Utah, 84119, USA
Toll Free: 1-800-221-7226

Executive Summary

Every marketing campaign is intended to create a specific response. Whether that desired action is to make a purchase, to refer a friend or to feel a particular way about a brand, the marketer's message has to reach the target audience and reach it at the right time.

To that end, marketers are consistently using email as a critical tool to distribute their messages, as several recent cross-industry studies have shown. For example, recently a leading independent research firm found that 94% of marketers use email as a communications channel. Meanwhile, numerous rigorous studies confirm that email plays an absolutely critical role when multiple marketing platforms (e.g. mobile, social media, digital, print, etc.) are used.

However, just as email's value as a cost-effective marketing tool has grown, so has the tendency for companies and individuals to implement technologies that reduce the volume and type of unwanted email being delivered into their email systems. Similarly, Internet Service Providers (ISPs) – organizations providing access to the Internet – are adopting methods to prevent the distribution of unwanted email.

While taking these steps is necessary to reduce the inconvenience and expenses incurred by receiving unwanted email, they pose a challenge to marketing campaigns. Even the most intrepid marketers can find themselves spending considerable amounts of money, effort and resources only to have their legitimate email marketing messages blocked – i.e. never reaching targeted audiences.

This whitepaper helps marketers increase the likelihood that their email messages will reach targeted audiences in a timely manner. By clearly identifying the five key challenges to getting email messages landing in the inbox – authentication, email reputation, being mislabeled as spammers by email recipients, being mislabeled as spammers by third-party software and server configuration – this paper provides marketers with a core understanding of deliverability. At the same time, the best practices included in this whitepaper are proven to help marketers address these deliverability challenges head on. The result: marketers' critical messages are more likely to reach their target audiences and achieve necessary campaign goals.

Introduction

Introduction

Who should read this whitepaper?

This whitepaper is intended for any marketer – in any industry – interested in increasing the success of their email campaigns.

What will you know / be able to do after reading this whitepaper?

By identifying issues that are central to increasing email deliverability – and practical steps to address them – this paper will assist marketers in better anticipating, planning for and reducing instances of email being prevented from reaching the inboxes of targeted audiences. The result: marketers' critical messages are more likely to reach targeted audiences and achieve necessary campaign goals.

Why has Thindata 1:1 prepared this whitepaper?

Since 1995, Thindata 1:1 has served as a valuable partner to senior marketers at some of North America's most respected and successful companies. In so doing, Thindata 1:1 has continuously developed, tested and refined email deliverability practices that have a positive impact on campaign success rates.

Thindata 1:1 recognizes that marketers have the right to take control of those issues – often identified as being the realm of the I.T. department or third-party suppliers – that have a dramatic impact on their campaigns' short- and long-term successes. By clearly and concisely identifying deliverability issues, this paper equips marketers to make better decisions in relation to email deliverability.

As a North American leader in delivering effective marketing strategies, tools and technologies, Thindata 1:1 is committed to helping marketing professionals by offering practical tools that make email marketing more successful.

Why is it important for marketers to address email deliverability?

Companies and individuals are implementing technologies that reduce the volume and type of unwanted email being accepted by their email systems. Internet Service Providers (ISPs) – organizations providing access to the Internet – are also adopting methods to prevent the distribution of unwanted email. While taking these steps may be necessary to reduce the inconvenience and expense incurred by receiving unsolicited email, they have a potentially disastrous impact for marketers. Specifically, marketers can spend considerable amounts of money, effort and resources only to have legitimate email messages blocked - i.e. never reach their targeted audience.

When should marketers use this whitepaper?

Marketers should use this whitepaper when:

- Setting goals for email marketing campaigns;
- Discussing the contributions of in-house I.T. departments to the success of email marketing campaigns;
- Discussing with Email Service Providers (ESPs) their capabilities and processes for ensuring email is delivered;
- Working with Internet Service Providers (ISPs) when discussing their role in the success of marketing campaigns; and
- Evaluating the success of email marketing campaigns.

Introduction (continued)

What research was conducted to prepare this whitepaper?

Thindata 1:1 drew on the experience of the following internationally renowned groups dedicated to investigating email deliverability issues and defining best practices:

- Email Experience Council (www.EmailExperience.org)
- Message Anti-Abuse Working Group (www.MAAWG.org)
- Email Sender & Provider Coalition (www.ESPCoalition.org)

Thindata 1:1 has also drawn upon its own considerable experience in developing successful email deliverability best practices for some of North America's largest and most influential companies in dozens of industries including: financial services, hospitality, travel/tourism, media, entertainment, government, retail and automotive.

Thindata 1-1
A TRANSCONTINENTAL COMPANY

Successful Email Delivery

Successful Email Delivery

Before tackling the email deliverability challenges facing marketers, it is important to briefly review what constitutes successful email delivery. To that end, we identify the key participants in the email sending/receiving process and how they are inter-related.

Marketer: The marketer is the leader of the email process. The marketer controls the domain name (i.e. email sending address), the list of intended recipients, the nature and layout of the content as well as the timing and frequency with which the email is sent. Combined, all of these elements – along with the sending email system configuration discussed below – shape the firm's email reputation. That reputation is a measure which is closely monitored by the second participant in the email chain, the Internet Service Provider (ISP).

Internet Service Provider (ISP): ISPs provide access to the Internet. However, for the marketer this access comes at a cost – a cost of compliance. ISPs establish, enforce and update rules of conduct dictating what constitutes a legitimate email and by extension a legitimate email sender. Marketers need to ensure that every email campaign complies with ISP rules to ensure their emails get delivered.

The most well known ISPs – including AOL, Hotmail/MSN, Rogers, Sympatico, Telus and Yahoo! – continually review emails looking for five critical pieces of information:

- Authentication of the email sender (i.e. Is the email being sent from an authorized server?)
- Presence on blacklists and/or content filters (i.e. Has the email sender been flagged as undesirable by a third-party anti-spam service?)
- Reputation of the sender's email server
- Configuration of the sender's email server
- Recipients' actions on previous messages (i.e. Have recipients flagged the emails from this sender by using a "Mark as Spam" button or equivalent?)

ISPs are continually monitoring and re-evaluating emails and email senders for this information. Adding another layer of complexity for marketers is that the criteria for each of these pieces of information change depending on the volume and type of email circulating the Internet. For example, if several potent email viruses are spreading across the Internet, ISPs can lower their acceptable thresholds to snare more dangerous email. To ensure that emails are accepted by ISPs, email senders must remain current and operate within these evolving restrictions.

Email Service Provider (ESP): While companies can manage their own email campaigns, ESPs play a critical role between the marketer and ISPs. ESPs translate ISPs' rules into best practices so that marketers can ensure their emails adhere to the codes of conduct that will enable successful email delivery. The ESP is in constant contact with ISPs in order to keep current on their evolving rules and restrictions. Full-service ESPs will actually monitor blacklists on behalf of marketers and resolve issues before they can have a negative impact on marketing campaigns. As such, ESPs serve as a central, trusted and convenient point of contact for ISPs as well as for marketers. Finally, an ESP provides a cost-efficient platform to send the marketer's emails to the ISP.

With this understanding of the participants and the roles they play in successfully delivering email, we now turn to the five challenges facing marketers' in their efforts to achieve email delivery. At the same time, we identify best practices to help marketers increase their email deliverability.

Thindata 1-1
A TRANSCONTINENTAL COMPANY

Five Challenges | Five Best Practices

Five Challenges | Five Best Practices

Challenge 1 | Making Sure Email Can Be Authenticated

When an email campaign is undertaken, emails are sent from the marketer's sending email server to the target audiences' receiving email server(s). But, before the email can be accepted, the receiving email server attempts to authenticate the email. That is, the server tries to confirm if the sender is the organization that it claims to be. This initial verification process – which, in traditional direct mail is comparable to checking the information contained in the return address on an envelope – involves the receiving email server using software to confirm if the sender of the email has the authority to distribute the message. To determine if the sending email source has that authority, the receiving server looks at lines of code – invisible to members of the targeted audience – for specific information:

- The Domain Name.
  Receiving email servers look to verify the domain name of the email sender. They draw upon the Domain Name System (DNS) which is similar to a phonebook that translates a "www" or URL address into an Internet protocol address approved for sending email messages. Two common pieces of information contained within the DNS that are used to authenticate email senders are text records called SPF (Sender Policy Framework) and Sender ID.
- Content.
  Receiving email servers can also use Domain Keys (DK) or Domain Key Identified Mail (DKIM) that validate the source of the email as well as the content within the message. These encryption-based technologies compare a token – i.e. a unique line of code – found in email against a sequence of numbers published in the senders DNS.

Best Practice: Taking steps to ensure that email can be authenticated is one of the prerequisites to ensuring that email is delivered to targeted audiences. Work with the I.T. department and/or a third party provider that is capable of publishing and maintaining SPF and Sender ID information within your DNS prior to any campaign. At the same time, evaluate the time, effort and expense associated with including encrypted tokens as these are becoming an industry standard.

For more information on Sender Policy Framework, Sender ID, Domain Keys and Domain Key Identified Mail, refer to the Resources section of this whitepaper.

Five Challenges | Five Best Practices

Challenge 2 | Maintaining A Good Email Reputation

Marketers are skilled at establishing, protecting and evolving a firm's reputation – in the eyes of clients, prospects, the media, suppliers and channel partners.

However, whether an email campaign is successful largely depends on the firm's email reputation as viewed by ISPs. Email reputation is based on the sender's history of email sending practices. Over time, ISPs monitor the flow of email through their system for the following types of information which contribute to a sender's email reputation:

- The length of time that a domain has been operating
- The number of invalid recipient email addresses to which email is sent
- The number of spam complaints submitted by email recipients
- The number of emails sent to addresses used to identify spammers
- Third-party information (e.g. presence on blacklists and whitelists)
- Configuration of the sending email server(s)

The more email a marketer sends that triggers questions along any of these dimensions, the more likely an ISP will automatically or manually monitor their domain. Eventually, that sender's actions can cause ISPs to temporarily filter or block their email. Persistent issues will cause the senders' emails to be permanently blocked.

Best Practice: In addition to using established domains, monitor your email campaign distributions for:

- Invalid emails. Review bounce-back files and remove inactive addresses after each mailing. Consider using closed-loop confirmation which involves sending an additional email to subscribers that prompts them to verify their interest in signing up for offers/ subscriptions. Develop a program that encourages inactive subscribers to verify their email.
- Complaints. Review the source of complaints, the length of time that complainants have been receiving email and the number of messages these recipients have received.
- Mail Server Settings. Review settings to ensure that the information contained within the Domain Name System (DNS) is current and correct. Clarify with the ISP acceptable thresholds for number of email retries, and the number of emails that can be delivered in a specific time period.
- Third-party Reputation Lists. Monitor blacklists for your mail servers, join a whitelist and build or outsource relationship-building with ISPs.

Five Challenges | Five Best Practices

Challenge 3 | Preventing Being Mislabeled As a Spammer by Email Recipients

Unlike many marketing tools – e.g. direct mail, billboard advertising, television and radio placement commercials – email provides marketers with instant and measurable feedback from targeted audiences. While such quick feedback can assist marketers to adapt elements of their campaigns – e.g. message, frequency, audience and offers – there is a potential downside.

More ISPs are providing email recipients – i.e. your targeted audiences – the means and opportunity to instantly report spam or junk-mail. While most email recipients will properly identify spammers and junk-mailers, some will mistakenly report legitimate email senders. This can lead to legitimate email senders being mislabeled as spammers and having their email messages blocked. The most common reasons being for such mislabeling are: recipients incorrectly identifying an email sender, recipients not recognizing an email sender, recipients being frustrated with an email sender, recipients wanting to quickly unsubscribe (i.e. be provided with a one click unsubscribe option) or recipients judging the content to be irrelevant .

- The length of time that a domain has been operating
- The number of invalid recipient email addresses to which email is sent
- The number of spam complaints submitted by email recipients
- The number of emails sent to addresses used to identify spammers
- Third-party information (e.g. presence on blacklists and whitelists)
- Configuration of the sending email server(s)

The more email a marketer sends that triggers questions along any of these dimensions, the more likely an ISP will automatically or manually monitor their domain. Eventually, that sender's actions can cause ISPs to temporarily filter or block their email. Persistent issues will cause the senders' emails to be permanently blocked.

Best Practice: To reduce the risk of targeted audiences mislabeling you as a spammer, have your ESP perform the following tasks regularly:

- Monitor feedback from ISPs and investigate the sources that have collected recipient information from promotional partners who may be having problems with unclear consent practices or forged subscriptions.
- Review subscriber opt-in processes to determine if subscribers are getting what they expect.
- Test and maintain your unsubscribe process ensuring that it takes effect immediately and is operating properly.
- Test you/your promotional partners' subscription and unsubscribe processes to determine if subscribers are getting what they expect.

1. According to a recent Email Sender & Provider Coalition (ESPC) and Ipsos' Email Survey, 80% of Internet users decide whether to click on the "Report Spam" or "Junk" buttons without opening the actual message.

Five Challenges | Five Best Practices

Challenge 4 | Preventing Being Mislabeled As a Spammer by Third-Party Software

Marketers need to contend with the fact that companies to whom they are sending emails can choose to manage large volumes of unsolicited email by using third-party filtering software. Such software can mistakenly mislabel legitimate email as undesirable and therefore block it. Furthermore, such software is used by many ISPs in conjunction with highly customized filters. Most third-party filtering software packages filter for:

1. **Email message content**
   Fully qualified domain names
   (i.e. addresses that fit the www.Company-Name.com format)
2. **Inclusion and frequency of keywords commonly found in spam messages**
   Email reputation (See Challenge 2 for factors that shape email reputation)

Best Practice: Reduce the risk of being blocked by third-party software by taking the following steps:

- » Update HTML code and content at least quarterly to keep current with evolving HTML standards – which can be found at w3c.org.
- » Use content-checking tools to avoid words that are often flagged as spam or spam-like.
- » Monitor your sender reputation
  (See Challenge 2 for factors that shape email reputation).
- » Use fully qualified domain names as hyperlinks in the body and address of email messages rather than Internet Protocol (IP) addresses which take the following form: http: //1.2.3.4/
- » Regularly monitor blacklists to determine if you or your ESP has been listed. Contact them to determine how to be de-listed recognizing that each list has different criteria for inclusion as well as delisting methods

Five Challenges | Five Best Practices

Challenge 5 | Configuring Email Servers to Meet Industry Standards

While marketers play a critical role in addressing the previous four challenges to email delivery addressing the final challenge tends to fall under the responsibility of the I.T. department. However, because the success of an email marketing campaign relies heavily on the final challenge – configuring email servers – the following highlights a handful of recommendations to help marketers in discussions with their I.T. department and/or Email Service Provider (ESP).

Best Practice: Follow industry standards for configuring email servers:

- Include and monitor distinctive points of contact such as email addresses for addressing general email inquiries (e.g. postmaster@abc.com) and reports of abuse (e.g.abuse@abc.com).
- Establish unique Internet Protocol (IP) addresses for each type of communication (e.g. corporate communications, marketing communications and transactional communications).
- Ensure software fixes/upgrades and applications are kept current.
- Adhere to the rules set out in your ESP's acceptable user policies.
- Adhere to the rules set out in your ISP's privacy policies.
- Assign responsibility for the proper use of reverse Domain Name System (DNS) – the process used by ISPs to verify that the server is properly labeled and authorized to send emails.

Next Steps

What comes after this whitepaper

This whitepaper provides an overview of deliverability issues and industry best practices to help marketers measurably increase the success of email campaigns.

Thindata 1:1 will follow this whitepaper with a series of publications developed to help marketers initiate, optimize and evaluate marketing success.

Resources

The following are links to additional information on the topics discussed in this paper.

Making Sure Email Can Be Authenticated

- SPF - http://www.openspf.org
- Sender ID - http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx
- Domain Keys - http://antispam.yahoo.com/domainkeys

Maintaining a Good Email Reputation

- http://www.senderbase.org/

Preventing Being Mislabeled As a Spammer

- http://www.spamhaus.org
- http://www.surbl.org
- http://www.uribl.com
- http://spamassassin.apache.org/
- http://www.emailstatcenter.com/Spam.html

Configuring Email Servers to Meet Industry Standards

- http://www.policycircle.com/rfc/

Legislation

- PIPEDA - http://www.priv.gc.ca/legislation/02_06_01_e.cfm
- CAN-SPAM - http://www.ftc.gov/bcp/edu/microsites/spam/business.htm

Thindata 1-1
A TRANSCONTINENTAL COMPANY

Email Deliverability

Best Practices Action Checklist

Email Deliverability

Best Practices Action Checklist

Use this best practices checklist to help your email marketing campaigns become more successful. Key deliverability action items identified in this whitepaper are outlined to assist you in discussions with your I.T. department and/or Email Service Provider (ESP).

	Best Practices Action Items	Ask Your I.T. Department	Ask Your ESP
To Authenticate Your Emails	Are you publishing and maintaining SPF and Sender ID information within your DNS?	✓	✓
	Are you including DKIM tokens in your DNS?	✓	✓
To Strengthen Your Email Reputation	Do you use well-established domains?	✓	✓
	Do you review bounce-back files and remove inactive addresses after each mailing?	✓	✓
	Do you use closed-loop confirmation for email subscribers?	✓	✓
	Do you have a program that encourages inactive subscribers to verify their email?		✓
	Do you review the source of email complaints?	✓	✓
	Is your DNS information current and correct?		✓
	Do you know the receiving ISP's thresholds for email retries?		✓
	Do you monitor blacklists and build relationships with ISPs?		✓
To Prevent Your Emails Being Mislabeled As a Spammer by Recipients	Do you monitor feedback from ISPs regularly?		✓
	Do review subscriber opt-in processes?		✓
	Do you test and maintain your unsubscribe process?		✓
	Do you test your promotional partners' subscription and unsubscribe processes?		✓
To Prevent Your Emails Being Mislabeled As a Spammer by Third-Party Software	Do you update your HTML code quarterly to keep current with evolving standards?		✓
	Do you use content-checking tools to avoid words that are often flagged as spam or spam-like?	✓	✓
	Do you use fully qualified domain names as hyperlinks?		✓
To Configure Your Email Severs to Meet Industry Standards	Do you include and monitor distinctive points of contact such as email addresses for addressing general email inquiries and reports of abuse?	✓	✓
	Do you establish unique Internet Protocol (IP) addresses for each type of communication?	✓	✓
	Are all software fixes/upgrades kept current?	✓	
	Do you adhere to the rules set out in your ESP's acceptable user policies?		✓
	Do you adhere to the rules set out in your ISP's privacy policies?	✓	
	Do you assign responsibility for the proper use of reverse DNS?	✓	✓

Thindata 911

Toronto

90 Eglinton Avenue East,

Toronto, ON, M4P 2Y3, Canada

Toll Free: 1-866-361-3522

Salt Lake City

1152 West 2240 South, Suite B

Salt Lake City, UT 84119, USA

Toll Free: 1-800-221-7226

Email us:
inquiries@thindata.com