The Grande Guide to

Email Deliverability & Privacy

Brought to you by

ELOQUA

What's a "Grande Guide"?

> We know what the typical day is like for marketers. After all, we are marketers ourselves. Between strategy sessions, impromptu meetings ("It'll just take a minute, really!"), and trips to meet colleagues and customers, you can barely find time to breathe – never mind keep up with the latest marketing trends. That's why we've developed the Grande Guide series. In the time it takes you to drink a cup of coffee, you can become proficient on a key marketing topic, in this case, email deliverability and privacy.

What is Deliverability and Privacy?

> Email deliverability is about maximizing the potential number of emails reaching the inbox. How well you do with deliverability depends on how your organization:
- ► Manages its email sender reputation
- ► Manages lists
- ► Ensures a quality database, such as where you get email addresses from and how you manage bounces

When it comes to email, privacy is about safeguarding the personal information contained in your mailing database. This includes honoring the opt-in/opt-out, data access, and data destruction wishes of the data subject.

Why Deliverability and Privacy Matter Today

Email deliverability and privacy matter more than ever. The first reason is that existing laws – and new ones on the horizon – up the stakes greatly for companies that don't comply with standards and regulations. Second, today's email marketers are finding it harder and harder to be heard. As a result, they need to master deliverability and privacy to rise above "noise" from social media, other email marketers, and even new techniques like word-of-mouth marketing.

A Return Path study found that 83% of delivery problems are caused by reputation issues.

Why Do We Need to Understand Deliverability and Privacy?

> Getting your message delivered is vital to revenue performance. After all, a slight increase at the top of the funnel can make a huge difference to your bottom line. And your ability to reach your prospects' inbox is tied to deliverability and privacy.

> As a marketer, you're continually collecting personal information through landing pages, web forms, third-party list providers and conference registrations. You're responsible for developing a comprehensive privacy policy and notifying individuals about how you will collect, use and protect their data. Plus, you need to do everything possible to reduce the likelihood of complaints, unsubscribes, bounces and spam traps.

> Your reputation as an email sender impacts your potential reach as a marketer. The following can earn you a poor deliverability score, which prevents your emails from reaching your desired target:
- ► Lack of adherence to an email privacy policy
- ► Poor list management
- ► Frequency and relevancy of sends
- ► Complaints from recipients
- ► Number of blocks
- ► Spam trap hits
- ► How people are engaging

> If you're not tracking who is active and inactive in your database, you'll keep sending emails to people who don't engage and your metrics will get skewed, making it hard to understand the effectiveness of your communications. After all, the more you know about your prospects, the better you will be at sending targeted, relevant emails.

> Furthermore, if your email is seen as spam, your IP address will be labeled as a spammer's IP, preventing you from getting into the inbox. According to Return Path, the world's leading email deliverability services company, more than 20 percent of opt-in email in North America does not make it to the inbox.

> Moreover, if you're not following regulations – such as the CAN-SPAM Act – in the country where you're conducting business, you're open to serious legal ramifications. For example, you need an explicit opt-in to send email to someone in the

> **Yet another reason to safeguard your prospects' privacy "A happy customer tells three friends. An unhappy customer tells Google."**
>
> *– SHIFT Communications CEO, Todd Defren* (@tdefren)

European Union, and in North America, you must provide clear options for opt-out.

> As soon as a subscriber's data is in your hands, you assume legal responsibilities with regard to collection, use, transfer, and the disclosure of and safeguards around that data — even if your organization is using a third-party data processor. This is a big problem for larger organizations, especially those with decentralized marketing; different departments tend to use different databases and maintain separate policies. In some cases, this practice can violate CAN-SPAM requirements, resulting in legal repercussions for your organization.

Deliverability and Privacy Basics (terminology, principles, key concepts)

> **Notice:** Data subjects should be given notice when their data is being collected.
> **Purpose:** Data should only be used for the purpose stated and not for any other purposes.
> **Consent:** Data should not be disclosed without the data subject's consent.
> **Data Subject:** Sometimes used in data protection legislation to indicate the person who is the subject of a personal data record.
> **Security:** Collected data should be kept secure from any potential abuses.
> **Onward Transfer:** Data can only be transferred to third parties that follow adequate data protection principles.
> **Disclosure:** Data subjects should be informed as to who is collecting their data.
> **Access:** Data subjects should be allowed to access their data and make corrections to any inaccurate data.
> **Accountability:** Data subjects should have a method available to them to hold data collectors accountable for following the above principles.
> **Data Controller:** A controller is any person or organization that decides how and why personal data will be processed.
> **Data Processor:** A person under the authority of a data controller who processes data on behalf of the data controller (e.g., an employee).
> **Safe Harbor:** Essential certification for transferring any data from the EU to anywhere in the United States for processing/use.
> **TRUSTe:** Third-party privacy monitoring and auditing service to ensure compliance and best practices such as adherence to U.S. Safe Harbor or said marketing practices.

Deliverability-related terms and principles:

> **Sender Reputation:** Sender reputations are based on your behavior as an email sender and consider complaints, hard bounce rates, blacklistings, inactivity, volume consistency and unsubscribe capabilities, to name a few.
> **Sender Score:** Although marketers may use the term synonymously with "sender reputation," sender reputation is a Return Path trademark. According to senderscore.org, sender reputation "measures a sender's behavior and the impact those behaviors have on email recipients and the sender's brand and email deliverability."
> **Complaints:** Complaints can happen for many reasons. For example, if the perceived email frequency is too much, the content is irrelevant, or the recipient cannot determine who sent the email. Complaints are the first thing to affect your sender score, and are considered a more important metric than many others since they are based on the recipients' perceptions of you.
> **Bounces:** A bounce is an email that gets returned to the sender because it was unable to reach the recipient's inbox. There are many types of bounces, but more common ones are hard, soft and blocks. A hard bounce generally means that the recipient's email address is invalid; these emails will never be delivered. A soft bounce often indicates a temporary issue preventing receipt of the email, such as a

© 2009 ELOQUA CORPORATION

restriction on the recipient's mailbox size. A block bounce typically indicates that filtering – whether content filtering, user filtering, complaint filtering, or other spam filtering – is impacting the deliverability of your email.

- ► It's illegal to harvest email addresses from websites to create a mailing list.
- ► If more than 10% of your list comprises bad email addresses, you can expect spam protection to block your emails. Industry average usually keeps the acceptable rate between 1 and 3%.

Deliverability and Privacy Best Practices

> Understand all capabilities of your email service provider. For example, does it manage global opt-outs automatically and in a compliant way, or remove hard bounces in a timely manner?

> Know the privacy laws where you do business. Get proper counsel.

> Get third-party certification as a trusted sender.

What is Sender Reputation?

Sender reputation is a score assigned to every mailing IP address (regardless of size or industry of the mailer) based on a combination of factors determined by your mailing practices, including content, frequency, and data sourcing. Your score is primarily based on three factors:

> Complaints (clicks on the Report Spam button)

> Infrastructure (reverse DNS and mail exchanger – or MX – record, volume/throttling, and bounce handling)

> List hygiene (source, quality and engagement)

Source: Return Path

Email Deliverability Best Practices
Step 1: Manage Your Reputation

A. Know Your Sender Score.

a. Measure it for free at http://www.senderscore.org. All scores are based on a scale of 0 to 100, where 0 is the worst and 100 is the best possible score.

B. Authenticate your Email IP Address.

a. Publish IP-based solutions like Sender Policy Framework (SPF) and Cryptographic solutions like DomainKeys Identified Mail (DKIM)

b. Create separate records for each type of email communication, such as promotional, newsletter and corporate.

C. Control Complaints.

a. Monitor complaint trends throughout each email campaign.

b. Avoid getting on blacklists. Monitor http://www.dnsstuff.com for your IP addresses, use the free lookup tool at http://www.mxtoolbox.com/blacklists.aspx, or see blacklistings via the Blacklist Monitor service from Return Path.

D. Gain Recipient Permission.

a. Only send to those who have explicitly requested email from you.

b. Target "neutral" contacts (i.e., those who have neither opted in nor opted out) with the goal of gaining permission.

c. Re-engage inactive contacts by confirming subscription status one or two times per year.

d. Strengthen the relationship with active opt-in contacts by soliciting feedback on the quality and frequency of your communications, and their communication preferences. Confirm preferences with the recipient and then comply.

e. Send only what the subscriber signed up to receive.

Step 2: Manage Your Email Distribution Lists

A. Validate List Sources.

- **a.** Don't buy or rent lists since they result in a higher number of complaints. Instead, organically generate your own leads and lists.
- **b.** If you do buy lists, make sure you trust the list provider regarding data quality and timeliness. Understand:
  - **i.** Source of data
  - **ii.** Age and last usage date
  - **iii.** How they monitor and remove complainers
  - **iv.** How they verify and maintain opt-in status
- **c.** Only send to email lists that have been recently compiled.
- **d.** Review Eloqua's Outside List Acquisition best common practices document.

B. Perform IP Warming Before Launching Campaigns On New IPs.

- **a.** Send to all addresses in a phased manner and then remove hard bounces.
- **b.** Confirm the list doesn't contain previously unsubscribed addresses.
- **c.** Use recent contact information only (i.e., less than 6 months old) and consider segmenting by domain for further cleansing.
- **d.** Use HTML with simple design, minimal images, and short copy.
- **e.** Review reports after each send to pinpoint problems.

C. Process Bounces.

- **a.** Remove hard bounces immediately.
- **b.** Keep hard bounces under 3% for each campaign.
- **c.** Monitor spam bounce reports and complaints over time to identify trends that help pinpoint changes in your marketing processes that may have hurt your reputation.

D. Filter on Recipient Activity.

- **a.** Segment by behaviors and target offers based on digital body language to reduce complaints and improve your reputation.
  - **i.** Filter contacts that have NOT opened or clicked on an email within the past 3 to 6 months. Send a separate campaign asking them to remove themselves from your list, manage their subscriptions, or tell you what you can do differently to raise their interest.
  - **ii.** After several unsuccessful attempts to obtain opens, clicks or unsubscribes, suppress contacts from future distribution lists. Focus on quality over quantity.

Email Certification: Does it Really Matter?
The email ecosystem is based on trust between subscribers, the mailbox provider or corporate administrator, and the sender or marketer (you!). We all want subscribers to enjoy a safe, protected and information-rich inbox experience. And we want to eliminate the possibility of subscribers reporting our email as spam or deleting it without reading.

Qualifying for third-party email sender certification rewards you for following sender best practices:

> Verifies that you are a trustworthy sender
> Ensures your email images and links are on by default
> Increases the likelihood of higher response rates
> Bypasses some filters
> Increases likelihood of making it into the inbox

Your Sender Score (available for free at www.senderscore.org is based on your sending practices, which determines if your messages will reach the mailboxes used by corporations, small businesses, and consumers using Yahoo!, Hotmail/ MSN and other free email services around the world. Mailbox providers use Sender Score data to sort senders into legitimate mailers who should reach the inbox and spammers who should be blocked.

Source: Tom Sather, Director of Prodessional Services, Return Path

Return Path's Sender Reputation Checklist

- ☐ Know your sender reputation by asking Eloqua or visiting www.senderscore.org.
- ☐ Track complaints and remove complainers by signing up for all feedback loops from the ISPs/ receivers.
- ☐ Dig into the root causes of why people complain – and adjust your email program to accommodate subscriber preferences.
- ☐ Determine if you are on any major blacklists and why.
- ☐ Authenticate with DKIM and SPF records. These are used by the various mailbox providers in proving trustworthy domains and are required for some whitelists. Check to see if you are authenticated: http://www.espcoalition.org/ senderid/
- ☐ Apply for as much sender certification (third-party and from the major ISPs) as you qualify for and can afford. Certification is reserved for the best senders and carries significant benefits.
- ☐ Understand the origin of and your relationship with everyone in your mail file. Keep only those subscribers who granted permission and are active.
- ☐ Align your permission policy with your business. Use stricter permission with high-frequency programs or with prospects who do not know you well.
- ☐ Be clear about frequency, message type and how data will be used at the point of subscription.
- ☐ Maintain a master calendar of messages sent to each subscriber, and optimize relevancy based on self-reported data as well as purchase behavior.
- ☐ Assign someone to regularly check your unsubscribe process, and your role accounts (e.g.: sales@, info@, etc.). Are the response techniques working properly? Be sure to forward customer requests for handling in a timely manner.

Step 3: Optimize Your Content

A. Reinforce Email Expectations.

- **a.** Clearly communicate your privacy policy and the type of content you send and when.
- **b.** Send a welcome message to new email subscribers with instructions on how to ensure the emails get delivered and the benefits of subscribing.
- **c.** Check in with contacts periodically to verify that they are satisfied with your content and highlight options for changing their communication preferences.
- **d.** Move your subscription management options to the top of your emails so they don't get overlooked.

B. Optimize Relevancy and Frequency.

- **a.** Use automated programs to test frequency and determine the optimal mix for your target audience.
- **b.** Ask subscribers for input and feedback on relevancy and frequency.
- **c.** Make sure you are clearly communicating your message—even with images turned off.

C. Review and Refine.

- **a.** Generate reports that provide insight into bounces, complaints, and unsubscribes.
  - **i.** Keep bounce rates under 3%. Monitor bounces by contact list, by email/email batch/email group and by those sent by automated email systems.
  - **ii.** Keep complaints under 0.01% by monitoring spam unsubscribes (i.e., contacts that reported your email as spam).
  - **iii.** Keep unsubscription rates below 1% by monitoring unsubscribe trends:
    1. How does this email campaign's unsubscribe rate trend against average performance? If there is a variance, pinpoint how this email differed from others in terms of list quality, content, etc.
    2. Is my unsubscribe rate trending upward? If so, investigate a possible frequency or relevancy problem.

Deliverability and Privacy Processes, Tools and Technologies

> **Feedback loops:** Get complaint reports and make adjustments to data sources as needed. Again, trend this data over time to identify changes in your process that may have caused the spike.
> **Bounce reporting:** Look at the percent of hard bounces (i.e., permanent failures) and keep this rate very low. Reporting needs to be comprehensive enough to tell you by email stream and by time frames the percent of hard bounces. Plus, look into reports and see the types of bounces and related messages as these might indicate a DNS issue.
> **Seed test:** Use an email-testing tool to see how your email will perform before sending to an actual list. Send the email to a bunch of live mailboxes intended to receive it and this will tell you the result and determine whether or not you have a deliverability problem. By sending to live, test inboxes but not to recipients, you'll get real-world deliverability feedback.
> **Spam filter check:** Email sent to specific spam filters (such as Postini, Barracuda, etc.) enables a real-world reputation check before you send live email.
> **Accreditation:** Pay neutral organizations for accreditation as an email sender. Return Path Certification is the most widely accepted accreditation program for email senders.

Deliverability and Privacy in Action

American Society of Civil Engineers

> The American Society of Civil Engineers experienced immediate results with Eloqua. According to the Society's Giselle Chasseloup, Coordinator of Collaborative Marketing, "Eloqua allowed us to increase outbound email volume from 130,000 to 1.5 million in 30 days, while maintaining an acceptance rate of more than 98 percent."

> Another Eloqua client produced a monthly email newsletter that regularly saw a 15% open rate and 1% click-through. After analyzing the subscriber list, the company found that 70% of its list was inactive. As a result, the open and click-through rates for active subscribers were much higher than the original numbers. By performing data quality and cleansing on the inactive subscribers, the company was able to gain more accurate insight into its response rates, while improving its overall deliverability.

What's Next in Deliverability and Privacy?

> **Privacy by design:** Privacy by design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation throughout product development, processes and support. In other words, it requires building in capabilities from the beginning that help marketers manage privacy concerns, for example, grouping contacts easily by region, segmenting data, etc.
> **Legislation:** At the time we published this Grande Guide, the EU is planning on full cookie opt-in requirements for mid 2011. In the US, a bill in discussion puts the onus on marketers to provide a full privacy policy for offline data, and could result in marketers needing to offer opt-in as the default. In other words, they would only be able market to people who opt in (which is similar to the process in Europe and Canada).
> **Deliverability:** We are seeing a move from IP to domain-based reputation. While the industry standard is SPF (i.e., IP-based authentication), there's a shift to DKIM (i.e., domain authentication). With DKIM, marketers can switch IPs without losing the reputation associated with the domain.
> **Social media raises visibility:** As social media continues to surface the topic of privacy and we become a more transparent and interconnected world, the issues of privacy and reputation will become increasingly important.

Digital body language is determined by the digital clues prospects leave behind when they engage with marketing assets.

© 2010 ELOQUA CORPORATION

Glossary/Resources

> **Deliverability.com:** News, rumors, and commentary from the email deliverability community - http://www.deliverability.com

> **Deliverability.com Blog:** posts on privacy - http://blog.deliverability.com/privacy/

> **Eloqua Email Deliverability Playbook**: http://img.en25.com/Web/Eloqua/EmailDeliverability_Playbook_1583.pdf

> **Eloqua Email Deliverability Resources:** http://www.eloqua.com/topics/email-deliverability.html

> **Eloqua Privacy Policy**: http://www.eloqua.com/trust/Privacy_Policy.html

> **Eloqua and TRUSTe Form Partnership**: http://www.marketwire.com/press-release/Eloqua-and-TRUSTe-Form-Partnership-1353331.htm

> **Email Reputation Score: Free Email Reputation Report from Sender Score**: https://www.senderscore.org/

> **Email Stat Center: The leading authority on email marketing metrics**: http://www.emailstatcenter.com/Deliverability.html

> **International Association of Privacy Professionals (IAPP)**: https://www.privacyassociation.org/

> **IAPP Glossary of Common Privacy Terminology**: https://www.privacyassociation.org/images/uploads/CIPP%20Privacy%20Glossary_0909.pdf

> **Messaging Anti-Abuse Working Group**: http://www.maawg.org/

> **Return Path**: http://www.returnpath.net/

> **Return Path's 2010 Email Deliverability Imperatives report** - http://www.returnpath.net/landing/emailimperatives2010/

> **SenderScore.org:** www.senderscore.org

> **U.S. Congress Planning Broader Email & Digital Marketing Enforcement and Regulatory Power for the FTC**: http://blog.emailexperience.org/blog/email-experience-council/0/0/us-congress-planning-broader-email-digital-marketing-enforcement-and-regulatory-power-for-the-ftc

> **What marketers might expect in 2010 around privacy:** blog post by Dennis Dayman of Eloqua - http://blog.deliverability.com/2010/02/what-marketers-might-expect-in-2010.html

Notes

© 2010 ELOQUA CORPORATION

Designed by
JESS3