2017 Email Marketing & Unsubscribe Audit

Benchmark research providing marketers, service providers and policymakers insight into enhancing the integrity and trust of email

Online Trust Alliance
an Internet Society initiative

Released December 6, 2017

TABLE OF CONTENTS

BACKGROUND

Since its formation in 2005, OTA has regularly published benchmark reports promoting awareness of such practices, while recognizing organizations which have demonstrated excellence in their commitment to online trust and user empowerment. Since earlier this year OTA is operating as an initiative of the Internet Society (ISOC), a global non-profit sharing a similar mission to promote the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society. Our work aligns with our goals for the Internet to be open, globally-connected, secure, and trustworthy.

Developing and accelerating the adoption of best practices to help bolster the integrity of interactive marketing and advertising is one of OTA's key initiatives. Email marketing continues to be an affordable and effective way to reach customers, maintain loyalty, inspire purchases and establish positive consumer brand perception.[1] While growth of the channel is encouraging, there are many factors that annoy consumers and can keep them from engaging with email marketing messages.[2]

In a continuing series of benchmark reports, OTA has initiated the 4th annual Email Marketing & Unsubscribe Audit, assessing the end-to-end user experience from signup through the mailing and unsubscribe process. With a focus on both compliance and transparency, OTA researchers have analyzed practices and offer prescriptive advice to help marketers provide consumers with choice and control over when and what messages they receive.

Working with multiple stakeholders, including input from the Federal Trade Commission, leading marketers, service providers and trade organizations, OTA developed a list of best practices and associated scoring criteria. These best practices also reflect the worldwide regulatory environment, including Canada, Australia and the EU, where there are increased calls for transparency and consumer control over email marketing. Leveraging learnings from the 2017 Online Trust Audit and the 2016 Native Advertising Transparency report, the criteria and scoring are re-evaluated annually to reflect current best practices. [3] [4]

The ultimate goal of this Audit is two-fold: 1) highlight and drive the adoption of email marketing best practices and 2) provide recognition to marketers who have moved from a compliance mindset to stewardship, putting users first. OTA recommends the adoption of the outlined practices to respect consumers' preferences. Failure to do so puts brands' reputation at risk and increases the risk of regulatory scrutiny. Conversely, putting consumers first is the foundation for industry innovation, growth and long-term vitality.

[1] For Many Marketers, Email Is Still King, https://www.emarketer.com/Article/Many-Marketers-Email-Still-King/1016393
[2] What's the Most Annoying Thing About Email Marketing?, https://www.emarketer.com/Article/Whats-Most-Annoying-Thing-About-Email-Marketing/1016480
[3] OTA Online Trust Audit, https://otalliance.org/TrustAudit
[4] OTA Native Advertising Transparency Report; Disclosures, Discoverability & Delineation, https://otalliance.org/native

EXECUTIVE SUMMARY

The 2017 Audit found that the vast majority of audited online retailers have embraced unsubscribe best practices, going beyond mere compliance, and have shown improvement since 2014 despite expanded and more stringent criteria. This year's audit was expanded to examine the entire email engagement process, from signup to receiving email to the unsubscribe user experience.

Consistent with the three previous reports, the Audit focused on the top 200 North American online retailers.[5] For each site, analysts measured and tracked the signup process and user experience, and after observing emails received for at least a month, each account was unsubscribed, and activity and compliance was monitored for a period of at least thirty days.

The primary objective of this report is to provide marketers, service providers and policymakers strategic insight about how to enhance the integrity of email marketing. Retailers achieving scores of 80% or higher received designation as "Best of Class."

For 2017, 67% of the top retailers qualified, a slight decline from 69% in 2016 and down from 75% in 2015. Nine of the audited retailers realized perfect scores – Blue Nile, Home Shopping Network, Lands' End, Musician's Friend, Sierra Trading Post, Stitch Fix, Talbots, Toys'R'Us and Walgreens.

> *"Marketers must not only focus on the relevancy of their campaigns, but most importantly the end-to-end engagement including the unsubscribe experience."*
>
> David Daniels, CEO and Founder The Relevancy Group

Despite the dip in "Best of Class" achievement, average scores actually increased slightly this year. OTA asserts that in order to maximize engagement, deliverability and brand reputation, the online marketing community needs to continue to put the user first and embrace the outlined practices.

As the regulatory landscape is evolving, marketers need to look beyond North America to anti-spam and data protection laws in other countries, most recently represented by the EU's General Data Protection Regulation (GDPR). Companies with an EU citizen or resident on an email list run the risk of potential fines of up to 4% of global revenues for violation of marketing, privacy and data protection practices.[6]

[5] Source: Internet Retailer®, https://www.internetretailer.com/top500/

[6] GDPR Overview, https://www.eugdpr.org/

KEY FINDINGS

Overall Results

- 67% of top retailers qualified as "Best of Class," scoring 80% or higher and being CAN-SPAM / CASL compliant, down slightly from 2016[7] [8]
- 9 retailers had perfect scores (vs. 12 retailers in 2016 and 23 in 2015). The primary cause for this decline is the new criterion this year requiring an encrypted session to the unsubscribe page.

Signup Practices

- 31% pop up a screen to solicit subscriptions and 28% make a promotional offer for signups, both down from 2016
- 11% require re-entry of the email address and 11% require account creation, both down significantly
- 3% used Confirmed Opt-In (COI) to verify subscriptions, down from 6% in 2016 and 11% in 2015
- Only 3% used CAPTCHA to reduce the risk of bot signups and "list bombing" (flat to 2016)

Email Authentication and Security

- Adoption of email authentication to help prevent business email compromise attacks, including spoofed and malicious email, was exceptional. 95% of retailers support SPF, 99% support DKIM and 60% have DMARC records. 33% use DMARC enforcement (a policy to reject or quarantine messages that fail authentication). These are all increases from 2016
- Opportunistic TLS adoption, which encrypts messages in transit between mail servers, thereby helping to prevent eavesdropping, nearly tripled, from 32% in 2016 to 90% this year

Mailing Practices

- 78.5% sent both a confirmation and newsletters/promotional messages, 18.0% sent only newsletters/promotional messages and 3.5% sent only a confirmation with no follow up
- Use of the unsubscribe header (which presents as a link or button in many consumer client mailboxes) grew to 92%, up from 89% in 2016
- The mailing cadence (frequency) varied from 4 per day to one per month. 19% of retailers automatically stopped sending (averaging 53 days) after no engagement, down from 28% in 2016

Unsubscribe Practices

- Clear and conspicuous unsubscribe links were observed in 76% of retailer emails, a continued decline from 81% in 2016 and 97% in 2015
- Readability of unsubscribe links continues to be a concern. 32% had unsubscribe text with contrast ratios below minimum W3C guidelines and 69% were below W3C enhanced guidelines
- Text size used for the unsubscribe link varied from 8 px[9] to 16 px, averaging 11 px
- For 76% of retailers, the word "unsubscribe" itself was the link to click

---

[7] CAN-SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/can-spam-rule

[8] CASL – Canada's Anti-Spam Law, http://crtc.gc.ca/eng/internet/anti.htm

[9] px is a unit used in web CSS design, https://www.w3.org/Style/Examples/007/units.en.html

- 51% of retailers presented the unsubscribe link in a standalone single-word footer, 28% presented it as part of a standalone sentence and 21% presented it within a paragraph of text, making it harder to find
- 52% used an encrypted session for the unsubscribe page, a new criterion this year. Encrypted sessions prevent user information, including the email address, from being sent "in the clear"
- 25% set an expectation for unsubscribe timeframe, ranging from one to 10 days, averaging 5.6 days

Unsubscribe Results

- 88% stopped sending messages immediately after the unsubscribe request was submitted (versus waiting the permitted 10 days), an improvement from 86% in 2016 and 83% in 2015
- Total violations of CAN-SPAM / CASL were 5.7% (11 retailers), flat to 5.9% (11 retailers) last year
    - Eight mailed 10 days past the unsubscribe request, a drop from 11 in 2016
    - Three did not list a physical address in their email as required by CAN-SPAM and laws in other countries (newly tracked this year)

SIGNUP PRACTICES

The testing process entailed visiting each retailer's website intending to subscribe to newsletters/promotions, and observing the entire process and user experience. In the 2017 Audit, signup practices were tracked and analyzed in greater detail than ever before. This added data will help create a baseline for future methodology and scoring. The analysis included any proactive efforts or incentives by retailers to recruit registrations, the required and optional data solicited for subscription and steps to validate the subscriber's email address. The results are shown in Figure 1 below.

SIGNUP PRACTICES		
	2016	2017
Invitation		
Signup on Home Page	-	97%
Signup at Top of Home Page	-	8%
Easy to Find	-	85%
Pop-Up Invitation to Subscribe to Email	34%	31%
Promo Offer on Screen for Signing Up	31%	28%
Signup Confirmation on Screen	89%	97%
Data Entry		
Required Email Address to be Entered Twice	16%	11%
Requested Additional Information	41%	36%
Required	-	28%
Optional	-	19%
Required Location	-	17%
Required Account Creation	20%	11%

Figure 1 - Signup Practices, 2016-2017

INITIAL INVITATION/ENGAGEMENT

Sites were observed for the discoverability and ease of signup and any signup incentives. OTA analysts also assessed the discoverability of the email signup, using criteria similar to the "Clear and Conspicuous" criteria for the unsubscribe link. While 85% of sites were deemed to have signups that were easy to find, 15% are missing an opportunity to serve consumers looking for engagement via email. While not measured, several sites made efforts to maximize subscriptions by including multiple subscription links – on the page header, within menu navigation and in the footer of the page.

As shown in Figure 2, 31% of retailers encourage signup through homepage overlays or pop-over windows, a drop from 34% last year. Most have a signup box or link on the home page, typically either in the upper (header) area (measured for the first time this year at 8%) or the lower (footer) area of the page.

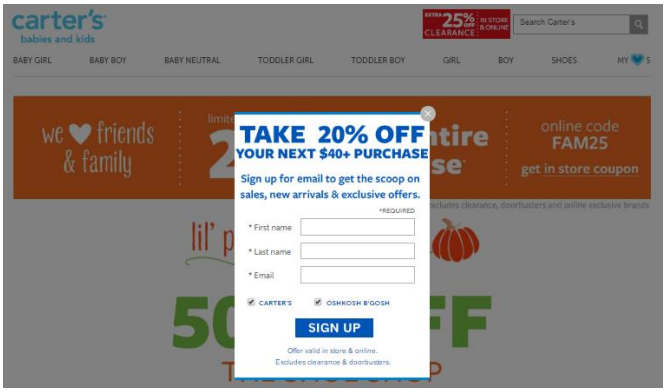


Figure 2 – Example of Pop-Up Window Inviting Subscription

Subscriptions were also solicited by offering a promotion or signup incentive (e.g., free shipping, discount on first order). Such incentives were offered by 28% of the sites (down from 31% in 2016) – 71% of these sites also made an offer via a welcome email, while 29% did not. Reiterating an offer or promo code both on screen and in an email is a recommended opportunity to engage and drive purchasers. Finally, on screen acknowledgment of a subscription lets the consumer know the request has been received (and is often used to set expectations for frequency or type of messages). This practice was used by 97% of retailers, a large jump from 89% last year. Disappointingly, 3% provided no confirmation after data was submitted.

DATA ENTRY

Entering an email address is all that is necessary to initiate a subscription, but as noted earlier there are important reasons to collect additional information benefiting the consumer and brand alike. These include: 1) verification of the address to avoid errors, 2) soliciting information (name, address, preferences, etc.) to tailor the subscription to consumers' needs and 3) to help maximize regulatory compliance, knowing the state/province and country of citizenship and/or residency.

This information not only enables marketers to easily segment their lists by country for additional compliance requirements such as re-verification of opt-in, but can tie to regional promotions and offers. OTA advocates that marketers embrace the concept of data minimization, only collecting and retaining the minimum amount of data where there is a clear and legitimate business purpose. For example, knowing the postal/zip code provides targeting capabilities without having the complete physical mailing address. The same principle applies to birthdays – if the business purpose is to send birthday-themed offers, month may be enough; if the business purpose is to filter out minors for legal compliance, a simple age assertion may suffice.

Overall, OTA noticed a distinct decrease in the amount and depth of interaction required for signups this year, likely in order to reduce friction on the front end of the process. Adoption was down in every tracked category.

OTA observed that 11% of retailers required the email address to be entered twice (down from 16%). OTA recommends requiring a user to enter the address twice to reduce the risk of users mistakenly typing in a wrong address, though some systems use a real-time verification or real-time hygiene solution to address this issue.

Thirty-six percent requested additional information about the subscriber (down from 41%), and only 11% required account setup (down from 20%, though this requirement clearly varies by business model). Of the

36% that requested information, 28% required additional information to complete the subscription and 19% asked for optional information (some requested both required and optional information, which explains why the total exceeds 36%).

Of significant concern is the low percentage of retailers requiring geographic information (only 17%), especially given that the EU's General Data Protection Regulation (GDPR) goes into effect in May, 2018, and has enhanced opt-in and data handling requirements for EU residents and citizens. It is possible that the retailer sites were keying off of location information in the browser and therefore did not ask for such information, but the consumer's citizenship or place of residence may be different than their location at time of signup.

As a best practice regarding the collection of additional information for enhanced customization, OTA advocates the prompting over time, with a clear emphasis that it is voluntary, not required. Conversely, requiring extensive information at initial sign up risks subscription abandonment. Creating the ability to "tune" emails provides users more relevant email communications. Maximum engagement can only be achieved when consumers receive email relevant to their interests, at a frequency aligned with their expectations.

SUBSCRIBER VALIDATION

Unauthorized and fraudulent email subscription abuse spiked in the summer of 2016 in "list or subscription bombing" attacks, causing consumers to receive hundreds of unsolicited emails within minutes. This effectively incapacitated users' email accounts and by utilizing email marketers and their service providers' infrastructures as an attack vector.[10] Though an attack of this scale has not been seen recently, to combat this risk OTA recommends that sites consider two simple practices.

CAPTCHA. The use of CAPTCHA (as shown in Figure 3) can help verify that the subscriber is a real person and not a bot. [11] While this doesn't prevent bogus subscriptions, it does reduce their scale since they can't be easily automated.

Confirmed Opt-In. OTA encourages the use of "confirmed opt-in" (COI), a longstanding practice in which an email is sent to the subscriber requiring them to click on a link to verify their subscription. Also referred to as double opt-in or roundtrip verification, this practice ensures that the recipient requested the subscription.

While COI can significantly reduce signup abuse, it can also decrease legitimate registrations since such confirmation email may be ignored, junked or discarded. Faced with list name acquisition costs and rising pressures to maximize lists, marketers have been reluctant to deploy, keeping COI adoption very low.

[10] List – Subscription Bombing https://wordtothewise.com/2016/08/subscription-bombing-esps-spamhaus/

[11] A challenge-response test to prevent bot signups, http://www.captcha.net/

Figure 3 – Example of CAPTCHA

Results from this year's subscriptions are shown in Figure 4 below. OTA has been tracking the use of COI for the last several years but this is only the second year to examine the use of CAPTCHA during the signup process. As noted, 3% of retailers used CAPTCHA to prevent bot signups (flat to 2016), while 2.5% of retailers used COI during the subscription process. Use of COI, which dropped by nearly half each of the last two years (11% in 2015 to 6% in 2016, now sub-3% this year), is concerning. Four sites that utilized COI last year no longer do, raising the risk of abuse. As a best practice to limit abuse, only two retailers utilize both CAPTCHA and COI during the signup process.

While such practices add signup friction, they also add value. Not only do they ensure more highly engaged signups, they also make a brand's site less attractive for abuse, help protect users' inboxes, and protect the brand's reputation, ultimately increasing user trust. Marketers might consider adding a callout or link during the signup process explaining why such practices are in place, further enhancing consumer trust of the sites.

SUBSCRIPTION VALIDATION PRACTICES				
	2014	2015	2016	2017
Confirmed Opt-In (COI)	7.9%	13.1%	6.0%	2.5%
CAPTCHA	-	-	3.0%	3.0%

Figure 4 - Subscription Validation Practices, 2014-2017

MAILING PRACTICES

Building upon the 2016 methodology, additional data attributes were captured and analyzed this year to better understand retailers' email practices. Areas analyzed included: subscription results, promotions within confirmation messages, use of email authentication and server-to-server encryption for newsletters/ promotional messages and the mailing "cadence" or frequency of mailing.

SUBSCRIPTION RESULTS

As shown in Figure 5, nearly 80% percent of marketers demonstrated the best practice of sending a signup confirmation and subsequent newsletter, on par with 2016 results. Eighteen percent skipped the welcome message and moved directly to newsletters/promotions. Nearly 4% sent only a confirmation with no follow up, indicating a breakdown in the system. This is an improvement over 2015 and 2016 (8.5% and 6% respectively), yet reflects lost opportunity for marketers who send a confirmation and nothing else.[12]

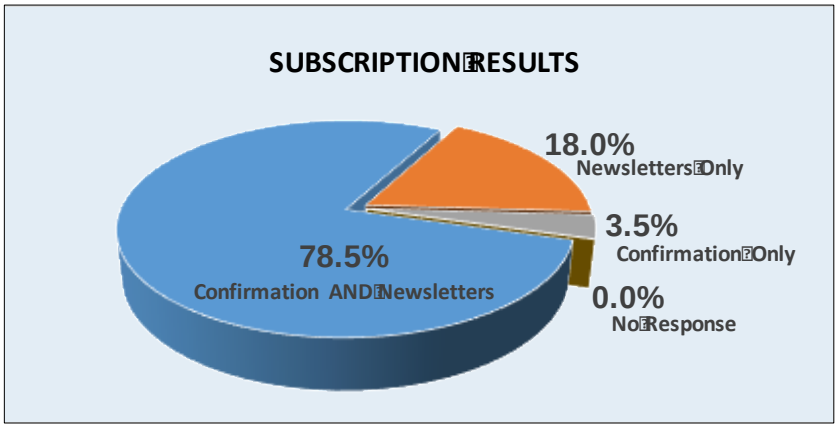


Figure 5 - Subscription Results, 2017

EMAIL AUTHENTICATION & SECURITY

Since its formation, OTA has been a strong proponent of email authentication to help counter fraudulent and malicious email, the primary tactic for phishing exploits. Over the past year use of such emails targeting business and government organizations has exploded. According to the FBI, Business Email Compromise has cost businesses over $5.3 billion between October 2014 and December 2016.[13]

Leading global email authentication standards include Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) and Domain-Based Message Authentication, Reporting and Conformance (DMARC). When deployed together they help ISPs and corporate mail systems (receivers) detect and prevent email spoofing while enhancing deliverability of legitimate messages.

[12] In instances where no confirmations or newsletters/promotions were received or only a confirmation was received, a second subscription using a different email address was completed to ensure that a mistake was not made. In most cases this addressed the issue, and email confirmations and newsletters started up as expected.

[13] Business Email Compromise, the $5B Scam, https://www.ic3.gov/media/2017/170504.aspx

DMARC builds on SPF and DKIM by: 1) allowing senders to publish a policy in their DNS instructing receivers how to handle messages which fail authentication and 2) receiving feedback reports for their domain(s). Opportunistic TLS encrypts the content of messages between email servers, enhancing the privacy of the message in transit, preventing eavesdropping by third parties including government agencies, malicious hotspots and others.

Leveraging the methodology of OTA's annual Online Trust Audit, a rigorous analysis of email authentication in retailers' newsletters/promotions was conducted. As outlined in Figure 6 the results were very positive, with adoption increasing in all areas. Due to the fact that newsletter mailings are generally managed by third-party email service providers (ESPs), authentication adoption for the email marketing domains is significantly higher than the same retailers' top-level (corporate) domains. The continued growth in adoption of DMARC policy assertions, which instruct receivers to quarantine or reject email that fails authentication, is key to preventing spoofing of those retailers' domains.

EMAIL AUTHENTICATION & SECURITY		
	2016	2017
SPF	94.1%	95.3%
DKIM	97.9%	99.0%
DMARC Record	50.5%	59.6%
Quarantine Policy	3.2%	4.7%
Reject Policy	21.8%	28.0%
Use of Opportunistic TLS	31.9%	89.6%

Figure 6 - Email Authentication & Security, 2016-2017

The positive surprise this year is the nearly tripling of opportunistic TLS adoption, which had been disappointingly low in 2016. Although TLS does not directly impact whether or not an email will land in the inbox, Google, Twitter, Microsoft and others have made a strong push for in TLS recent years, to the point where Gmail highlights messages without TLS with an unlocked red padlock, as seen in Figure 7. This can negatively impact the user experience, open rates and user engagement. This points out the influence of widespread consumer services such as Gmail on industry adoption, and OTA applauds this dramatic move by email service providers to adopt opportunistic TLS over the past year.

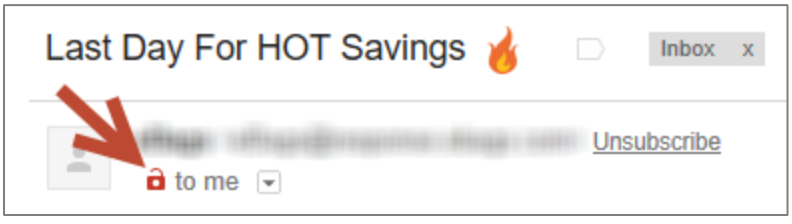


Figure 7 – Example of Gmail TLS Indicator

MAILING CADENCE

New in the 2017 Audit, the cadence of mailings, as defined by the frequency and continuation of sending email, was tracked. It should be noted that the OTA mailboxes used to receive messages were configured not to download images. Combined with not actively opening the messages until weeks later, some marketers may have viewed our test subscriptions as unengaged and responded accordingly by throttling back the cadence or stop sending altogether.

Most retailers mailed with a consistent cadence, which varied from four messages per day to once a month. However, more than one-fourth (54) reduced mailing frequency over time, likely in response to the non-engagement. This is triple the number seen in 2016, indicating that retailers are tuning their programs to be more sensitive to user engagement (or lack thereof). In one case a retailer started with daily messages, but then backed off to one per week after 60 days. Another sent messages every two days for two weeks, then successively backed off, ultimately reaching a weekly cadence after 90 days.

In addition, 19% of retailers actually stopped sending entirely (without an unsubscribe) after a period of time, which varied from 4 days to 120 days, averaging 53 days. This is down from 28% of retailers in 2016 who automatically stopped sending. The combination of increased cadence adjustments and less automatic cessation of messages seems to indicate that retailers are favoring fine tuning of their messages over hard stops.

UNSUBSCRIBE PRACTICES

The unsubcribe process and associated user experience have represented the primary analysis and reporting focus since the inception of this report. In conjunction with the email marketing community and consumer advocates, OTA has developed the list of scored best practices which we believe maximize user choice and control over the unsubscribe process. The criteria and description of the twelve scored practices are outlined below. The following findings and analysis in are presented in three stages: 1) transparency – the disclosure, discoverability and delineation of the unsubscribe option in email messages, 2) the unsubscribe process itself and 3) the unsubscribe results including compliance.

It should be noted that the Federal Trade Commission (FTC) issued a request for comments on CAN-SPAM in July, reflecting back over a decade since CAN-SPAM was enacted. [14] The FTC requested input regarding possible changes to reflect today's technology and environment and possible suggestions on how to improve the Rule. OTA, in collaboration with many members, submitted a response in August.[15]

SCORED UNSUBSCRIBE BEST PRACTICES

1. **Clear and Conspicuous Link.** Opt-out copy and link should be "clear and conspicuous" and not buried among long paragraphs of legal language. The opt-out should be visible from the last sentence of the body of the email, minimizing vertical space between the end of the body copy and the link, and a different color than surrounding text to help identify it as a link. The user should not be forced to download images in order to identify the unsubscribe link.
2. **Commonly Understood Terms.** Commonly understood terms such as "unsubscribe" or "opt-out" should be used. Avoid terms such as "Click here to Modify your Subscription Practices" as it may be perceived as an attempt to obfuscate the suppression link. These tactics tend to undermine brand trust and integrity. OTA recommends separate links which call out the key preference options by name even if the links all lead to the same preference page. For example, the following terms can all be included in the footer of an email and lead to the same page: unsubscribe, change email/physical address, reduce frequency or update profile. Ideally each should have links to allow consumers to update their preferences.
3. **Size/Readability.** The unsubscribe text should be both discoverable and able to be easily read by recipients of all ages and on all devices. As a general guideline, unsubscribe links should be no more than 2 points smaller than the body copy of the email and no smaller than 10-pixel font size (10 px in CSS design terms) and not require the user to move the mouse over the text to find the link. The font color should be readable with adequate contrast from the background, ideally in a different color and style than the body copy.

[14] FTC request for comments on CAN-SPAM, https://www.ftc.gov/system/files/documents/federal_register_notices/2017/06/can-spam_published_frn_6-28-17.pdf

[15] OTA reply to FTC call for comments on CAN-SPAM, https://otalliance.org/system/files/files/initiative/documents/online_trust_alliance_can-spam_rfc_response.pdf

Though historically many email and websites have had white backgrounds with dark text, many have recently switched to light grey backgrounds with greys or blues for their type. Black text on a white background has a contrast ratio of 21:1 – the maximum contrast possible. The best practice for small type is a minimum contrast ratio of 4.5:1 (and 7:1 for enhanced contrast) so that the visually-impaired can still see text.[16] In addition, given LCD technology and high definition screens, designers are using increasingly thinner fonts, which can be difficult to read on smartphones or tablets. Designers need to recognize that a wide variety of users of all ages will be interacting with these messages and many have increased vision requirements.

4. **Unsubscribe Header.** All email should include the "unsubscribe header." Senders should adopt the List-Unsubscribe mechanism within the header of each message as described in RFC 2369.[17] Including the header allows ISPs and automated unsubscribe services to easily identify your opt-out mechanism. Gmail, Microsoft Outlook, Yahoo! Mail and other leading ISPs and mailbox providers display an unsubscribe button to the user in the user interface when a List-Unsubscribe header is found. Increasingly, mobile email clients such as Outlook also present the header as a link as well. The use of this header will help reduce complaints because your recipients will be able to easily and reliably unsubscribe.

5. **Opt-Out of All Email.** An easy mechanism or choice to opt-out of all email should be provided. If a marketer has multiple email programs, they must have an option to opt-out of all email as well as the individual email campaigns and programs. Related best practices dictate that where third-party publishers are undertaking the campaign, a second link unsubscribing from the publisher should be placed below the advertiser's link.

6. **Confirmation Web Page.** Serve an unsubscribe confirmation web page. Thank subscribers for participating in your program with a simple statement such as "We're sorry to see you leave our newsletter" and offer a (re)subscribe if they made a mistake. Do not send a confirmation email as it can be a violation of CAN-SPAM and risk further alienating consumers. Consider providing alternative channels such as Facebook, Twitter, YouTube, etc. for consumers to maintain a relationship with your brand.

7. **Branded Unsubscribe Page.** An unsubscribe confirmation web page should be clearly branded – ideally like the website – to eliminate the confusion generated by an unbranded page. Make it clear that site visitors are in the right place. Include branding and links back to your home page and privacy policies.

8. **Pre-population of Unsubscribe Address (new in 2017).** During the unsubscribe process, the address being unsubscribed should be pre-populated (or clearly listed) on the unsubscribe page to avoid user confusion or mistakes. Many users now feed multiple email addresses into a common inbox, making it difficult for them to remember or determine which address they used to subscribe to a given email. Pre-populating the address also protects against data entry mistakes.

---

[16] See "Distinguishable" section of W3C Web Content Accessibility Guidelines (WCAG) 2.0 https://www.w3.org/WAI/WCAG20/quickref/

[17] IETF RFC 2369 published July 1998 https://tools.ietf.org/html/rfc2369

9. **Preference Center and/or Opt-Down.** Users should be directed to a preference center to unsubscribe, opt-down or make other changes, but in doing so the unsubscribe choice cannot be obfuscated. Users cannot be required to log in with a password to unsubscribe. An opt-down option gives users a choice to reduce the frequency of emails that they receive. Similarly, consumers can be offered the ability to choose what type of messages to receive (e.g., newsletters vs. promotions vs. product information). Note it is recognized that small companies and low frequency senders may not have the scale or size to offer such options.

10. **Optional Customer Feedback.** A simple form should be offered during the unsubscribe process to allow customers to provide feedback. This allows companies to refine their email marketing program to help prevent future opt-outs. A simple check box list can be used to determine why customers are unsubscribing. Remember this cannot be required as it would violate CAN-SPAM. A common treatment is to present the comment boxes below or after the opt-out option. Do not send a follow up email asking why they unsubscribed since it would be a violation of most if not all anti-spam regulations. Allowing the customer to provide feedback can help determine specifics about their dissatisfaction (e.g., frequency, content, timing or other aspects of the email marketing program, including practices by third party affiliates and publishers).

11. **No Delay on Removal.** Unsubscribes should be removed without delay. While CAN-SPAM and CASL both allow up to 10 business days for suppressing mailings, OTA recommends users be removed and added to suppression lists as soon as possible. Waiting 10 days and sending additional email will only reduce user engagement and possibly lead to an increase in spam complaints. Note that Australia, New Zealand and other countries require businesses honor an unsubscribe request within five working days.

12. **Encrypted Session for Unsubscribe Page.** Unsubscribe pages should be encrypted by default to protect the information being transmitted, which by definition includes the user's email address and potentially other sensitive information as they navigate a preferences page or other unsubscribe interaction. This ties to OTA's and the Internet Society's advocacy for "Always On SSL" or "HTTPs Everywhere," encrypting every page of a site.

RELATED BEST PRACTICES

While not scored, the following practices should be adopted to help maximize regulatory compliance and campaign performance.

1. Unsubscribe links should be operative for a period of no less than 60 days (CASL requires 60 days and CAN-SPAM specifies 30 days). As consumers may move outside of the U.S. marketers are best suited to adhere to these standards.

2. Testing & ISP Feedback Loop Data (FBL) should be utilized. With FBL data ISPs can help identify problems with email campaigns that can drive unsubscribes and damage deliverability. Test campaigns on a range of devices and platforms for optimal rendering.

3. **Email and all suppression lists should be encrypted**. As with any data, mailing lists can be exposed via breaches or accidental disclosures. As lists typically include sensitive or protected data, data loss incidents of email lists are increasingly subject to foreign, federal and state data breach legislation. Hashing and encryption should be considered to minimize the risk of list abuse, while aiding in maintaining security and integrity of all lists, including those "in motion" and "at rest." This includes any third parties that handle the information. See OTA best practices, including those in the Cyber Incident & Breach Readiness Guide as well as the IoT Trust Framework.[18]
4. **A mechanism for users to update their data should be provided**. Users may change their email and physical address but wish to retain their profile data. This also ties to the ability to understand the user's citizenship or residency for compliance with appropriate data protection and breach laws and regulations.
5. **Email Authentication** should be implemented to help protect brands from spoofing and forgery. The combined use of SPF, DKIM and DMARC across all sub and parent level domains helps to provide ISPs, mailbox providers and receiving networks the ability to detect malicious email and prevent it from being delivered to users' mailboxes.[19]
6. **CAPTCHA and Confirmed Opt-In (COI)** should be used to verify subscribers. CAPTCHA reduces the risk of bot signups and COI ensures that subscriptions are legitimate. Combined they protect consumers and marketers/service providers from being used for "list bombing" and similar attacks.
7. **State/Province and Country should be captured** during the signup process. This helps marketers understand which regulatory environments apply to their subscriber base. This is especially important with the General Data Protection Regulation (GPDR) going into effect in the EU in May, 2018.

DISCLOSURE, DISCOVERABILITY & DELINEATION

Adoption of best practices in the message itself increased in all but one area – Clear and Conspicuous unsubscribe links – but it is the most important overall indicator of discoverability. The "clear and conspicuous" criterion actually takes into account a combination of factors related to the discoverability of the unsubscribe link and has been on a continuous decline since 2015. The ease with which users can find the link is impacted by placement, surrounding text and graphics, color/contrast/size and use of terms.

AUDITED & SCORED BEST PRACTICES IN THE MESSAGE

	2014	2015	2016	2017
Easily Read / Size	96.8%	98.4%	92.6%	93.8%
Commonly Understood Terms	86.2%	94.0%	88.8%	91.7%
Unsubscribe Header	75.7%	85.2%	88.8%	92.2%
Clear and Conspicuous	80.4%	97.3%	81.4%	75.9%

Figure 8 - Adoption of Scored Criteria in the Message, 2014-2017

[18] Cyber Incident & Breach Readiness Guide, IoT Trust Framework – https://otalliance.org/Incident, https://otalliance.org/IoT

[19] Email Authentication & DMARC resources – https://otalliance.org/eauth

Though data detailing the method by which the unsubscribe link is presented has not been tracked in prior years, the use of standalone single-word footer menus to present the unsubscribe link seems to be growing, effectively creating a divergence in approach – the best are getting better by making the link even easier to find, while the rest are obscuring the link even more through placement, design choices and terminology.

To explore this issue, additional data was collected this year. One set of data looked at the placement of the link (standalone single-word footer menu vs. standalone sentence vs. part of a paragraph), another looked at the exact size and color contrast of the unsubscribe link text and the third looked at whether the link to click was actually the word "unsubscribe" (or equivalent) vs. other generic words somewhere else in the sentence. The results are explained in the following paragraphs.

Unsubscribe Link Placement. As seen in the examples in Figure 10, there are a variety of ways to present the unsubscribe link, ranging from easy to somewhat difficult to find. Figure 9 shows the breakdown of the different approaches, and though this data was not tracked in 2016 there seemed to be a decided move toward use of standalone footers compared to previous years. This is encouraging since it makes it easier for consumers to find the link.

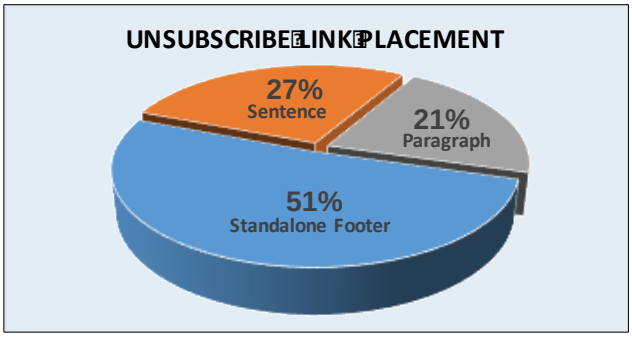
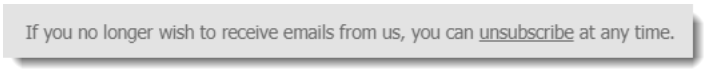
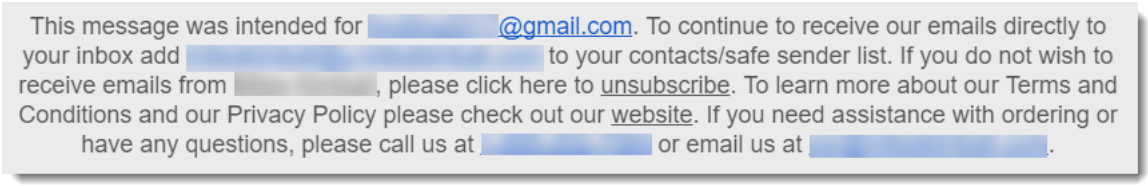


Figure 9 – Unsubscribe Link Placement, 2017

Example A – as part of a standalone footer



Example B – as a standalone sentence



Example C – in a paragraph

Figure 10 – Examples of Unsubscribe Link Placement

Unsubscribe Link Text Size. Text size for the unsubscribe link was also tracked, and the breakdown is shown in Figure 11. From a scoring standpoint, sizes less than 10px did not receive credit, and though 10px text can be difficult to read (depending on the contrast), it was given credit for adequate size. Text larger than 10px was also given credit and became successively easier to read. For reference, 12-point type in print equates to 16px text on a website. Ideal text size is a widely debated topic in web design circles, but most experts recommend type sizes in the 12px-16px range for ideal readability of body text.

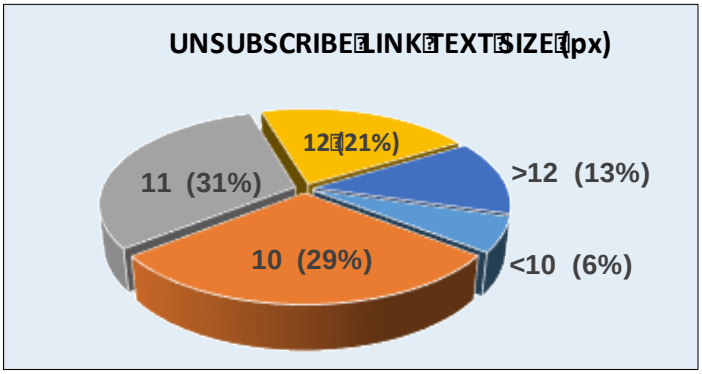


Figure 11 – Unsubscribe Link Text Size, 2017

Unsubscribe Link Contrast Ratio. The contrast ratio for unsubscribe link was also measured for the first time this year, and though it is not the only measure for discoverability (placement, size, text treatment and contrast with surrounding text all play a role), it is telling. According to the Web Content Accessibility Guidelines created by the W3C, nearly one-third (32%) of unsubscribe links had a contrast ratio below 4.5:1 (17% were below 3:1), so were under even the minimum guideline. Sixty-nine percent of the links were below the enhanced guideline of 7:1. [20]

"Unsubscribe" as Link. Another factor impacting discoverability is the location of the link itself within the text. Therefore, OTA analysts tracked the word that was used as the unsubscribe link. In total, 76% of messages used the word "unsubscribe" or "opt-out" itself as the link to click (only one retailer used "opt-out"). The remaining messages used "click here" or other words in a sentence as the link. In general, this makes the link harder to find since the entire sentence must be read to understand what the "click here" refers to, and the bottom of most marketing messages has several clickable links for different purposes. OTA encourages all marketers to utilize the word "unsubscribe" (or equivalent) as the clickable link.

Combining all these elements, assessment of "clear and conspicuous" presentation of the unsubscribe link was conducted. Some examples of messages that failed are shown in Figure 12.

If you'd like to unsubscribe or receive fewer marketing emails, please click here. To read our privacy policy, please click here.

Example A – link not clear and conspicuous (this is part of a large paragraph)

If you wish to no longer receive marketing and promotional emails from [redacted], please click here. Note that you may continue to receive transactional and operational emails from us.

Example B – poor terms

Figure 12 – Examples of Poor Disclosure, Discoverability and Delineation

[20] WCAG 2.0 Quick Reference Guide (see 1.4.3 and 1.4.6), https://www.w3.org/WAI/WCAG20/quickref/

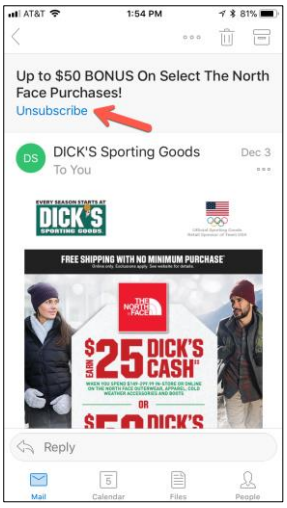


Figure 13 – Example of Unsubscribe Header Link in Mobile Client

Another jump in adoption of use of the unsubscribe header was seen this year, reaching 92%. Marketers should take advantage of this capability since most consumer mailboxes will render this as an easy to find link. This header is now also being presented as a link in many mobile clients, further increasing its value. Examples are shown in Figures 13 and 14.

Unfortunately, since marketers can't know which email client will be used to actually view the message (even if the user's address is a Gmail, Microsoft or Yahoo address), they cannot count on the header-generated link and need to make sure the unsubscribe link in the message itself is easily discoverable.

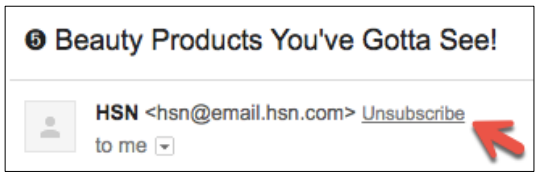


Figure 14 – Example of Unsubscribe Header Link in Gmail

UNSUBSCRIBE PROCESS

Figure 15 below lists best practices for the unsubscribe process. These include 1) the ability to opt out of all email, 2) landing on a branded page confirming the unsubscribe, 3) pre-population of the unsubscribe address, 4) presentation of a preference center / opt-down choice during the process and 5) soliciting of feedback regarding their reason(s) for unsubscribing. Each has its place, from the single-step confirmation of the request through choice and control for the consumer.

AUDITED & SCORED BEST PRACTICES
UNSUBSCRIBE PROCESS

	2014	2015	2016	2017
Opt-Out All Email	93.7%	97.3%	99.5%	99.5%
Confirmation Web Page	95.2%	94.5%	98.9%	100.0%
Branded Page	85.7%	90.2%	92.6%	93.3%
Pre-Populated Unsubscribe Address	-	*90.7%*	*92.0%*	95.3%
Preference Center and/or Opt-Down	91.0%	61.7%	58.5%	58.5%
Preference Center	-	55.7%	37.8%	37.8%
Opt-Down	-	44.8%	33.0%	33.2%
Optional Customer Feedback	24.9%	24.0%	22.9%	20.2%
Encrypted Session to Unsubscribe Page	-	-	-	51.8%

Figure 15 - Adoption of Scored Criteria in the Unsubscribe Process, 2014-2017 [21]

[21] Note that in 2014 retailers received credit if there was a preference option in the email footer. Starting in 2015, credit was given only if preference center / opt-down was offered as part of the unsubscribe process. Pre-populated unsubscribe address data from 2015 and 2016 is shown in italics since it was tracked but not a scored criterion.

Overall Experience. As in previous years the unsubscribe experience ranged from abrupt, non-branded one-click interaction to elegant, branded experiences that walked seamlessly through various preference choices and solicitation of feedback. Several retailers presented a "please subscribe" pop-up during the unsubscribe process, which is clearly a contradiction of purpose (this likely happened due to lack of cookies on the test computer, but this should be suppressed so as not to annoy or confuse the user). Examples of extremes in experience are shown in Figure 16 below.

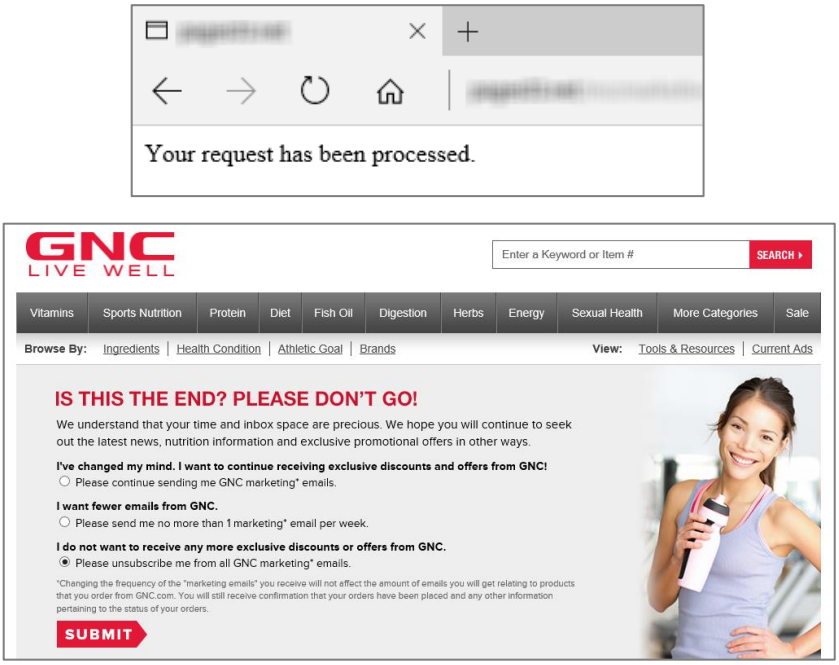


Figure 16 – Contrasting Examples of Branding in Unsubscribe Pages

Pre-Populated Unsubscribe Address. New to the scoring criteria this year is the pre-population of the unsubscribe address, which is convenient for consumers and reduces errors, frustration and complaints. More than 95% of retailers already use this practice. A few retailers offered the option to reply with "unsubscribe" in the subject line, but this may not work since the user's current email box may different than the one used for the subscription. As a result, the user may continue to get email even though they believe they have unsubscribed. In the scoring of future audits, this best practice will likely receive additional weighting

Encrypted Session to Unsubscribe Page. Also new this year is tracking of whether the session to the unsubscribe page is encrypted. In this initial assessment, 52% of retailers encrypted sessions to the unsubscribe page, and though this seems low, it is higher than the 39% adoption of "Always On SSL" or "HTTPs everywhere" for the main websites of these same retailers. Many unsubscribe pages are served by the retailer's email service provider (ESP), so they should ensure that such pages are set to use encryption.

Branded Unsubscribe Page. Ninety-three percent of retailers used a branded unsubscribe page this year. Even within branded pages the look and feel varied dramatically – marketers should periodically test and evaluate the user experience to ensure that the unsubscribe process represents the branding experience they desire.

Because the unsubscribe request is often handled by ESPs, integration can be challenging, though most ESPs offer a way to extend the corporate branding experience into the unsubscribe process.

Preference Centers/Opt-Down. Even though the list of retailers was slightly different this year, the use of preference centers and opt-down options was precisely flat to 2016. As mentioned last year, there are now other means to determine consumers' interests without use of a preference center, though OTA encourages marketers to maximize user choice and control to minimize list abandonment. In addition, rather than waiting for a user to unsubscribe, marketers should consider providing inactive subscribers a link to a preference center.

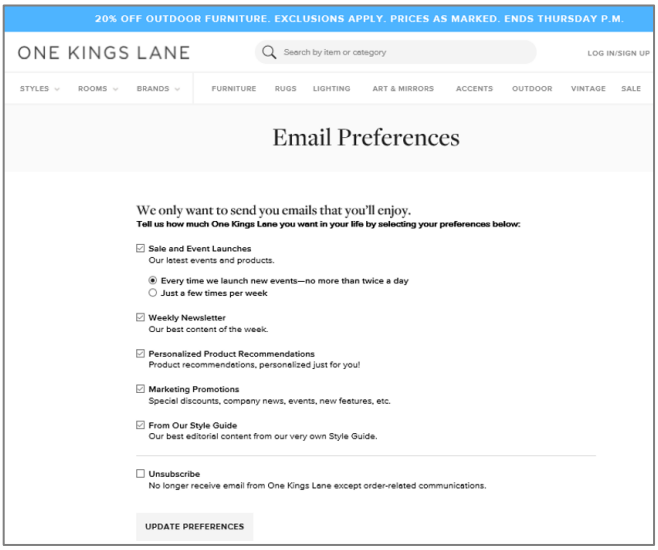


Figure 17 – Example of Preference Center / Opt-Down Choices

Figure 17 is an example of a preference center / opt-down presentation that is intuitive and concise, offering the consumer an easy way to adjust choices instead of taking the "all or nothing" unsubscribe approach. For many retailers the "Unsubscribe" and "Email Preferences" links in the email take consumers to this type of page.

Optional Customer Feedback. Adoption was flat or increased in all but "Optional Customer Feedback", which continued its slow decline. Soliciting this type of feedback ("Why did you leave?", "How can we improve your experience?", etc.) is a great opportunity to help fine tune content and processes to increase retention and reduce unsubscribe rates and spam complaints, though it must be tested for user engagement.

Setting Unsubscribe Timing Expectations. For the first time, analysts captured expectation-setting regarding time done by retailers during the unsubscribe process, and 25% of them gave a specific timeframe (e.g., "You have been unsubscribed. Please give us 3 days to honor this request."). The stated timing ranged from one day to ten days, averaging 5.6 days. OTA applauds this move to go beyond compliance by setting an expectation tighter than the required ten days and to proactively communicate the expectation to consumers. Nearly all retailers who made such a commitment met or exceeded it – the few who did not failed to honor the unsubscribe request at all. This element was not scored, but may be factored into future reports.

UNSUBSCRIBE RESULTS

These criteria include the honoring of the unsubscribe request (immediately versus within regulatory requirements) and whether the company sent an unsubscribe confirmation email. Points were awarded for companies that honored requests immediately (a one-day grace period was used to allow for cases where campaigns were queued up prior to an unsubscribe request), points were deducted for companies who sent an unsubscribe confirmation email, and companies were disqualified if they violated CAN-SPAM, CASL or other regulatory guidelines. For the Audit, a "violation" was defined as having a broken unsubscribe link, no physical address in the email or continuing to send email more than 10 business days after the unsubscribe request was submitted.

As shown in Figure 18, immediate honoring of unsubscribe requests grew to 88%. This shows that the vast majority of retailers go beyond compliance to stewardship, recognizing that sending messages after the unsubscribe request has no upside and can only annoy consumers, increasing spam complaints.

Figure 18 also shows the percentage of companies who sent an unsubscribe confirmation email or who did not honor the unsubscribe request. Sending of an email to confirm an unsubscribe request received penalty points but did not disqualify a retailer from consideration for "Best of Class." Use of this practice flattened out at 2.7%. By itself an unsubscribe email confirmation may not be a compliance issue. It depends on the content of the message – attempts to re-engage or incent the subscriber can be considered a violation.

UNSUBSCRIBE RESULTS				
	2014	2015	2016	2017
Unsubscribe Confirmation Email	4.8%	2.7%	2.7%	2.1%
No Delay on Removal	82.5%	83.1%	85.6%	88.1%
Violate CAN-SPAM/CASL (total)	10.9%	7.1%	5.9%	5.7%
Failed to Honor Unsubscribe	-	1.6%	5.9%	4.1%
Broken Unsubscribe Link	-	5.5%	0.0%	0.0%
Physical Address not Listed in Email	-	-	-	1.6%

Figure 18 - Unsubscribe Results, 2014-2017

Of the four companies who issued an unsubscribe confirmation email, all confirmed the unsubscribe request. Only one set an expectation for how long it would take. Two of the four offered a link to "change email preferences" if the recipient changed their mind or had unsubscribed in error. The other two were purely a confirmation with no means to re-subscribe. None made any promotional overtures.

The number of retailers that failed to honor the unsubscribe request dropped to 4% (8 retailers) from 6% (11 retailers) last year. It appears that one changed ESPs during this testing window since they honored the unsubscribe for more than 30 days and then started up again, sending from a different subdomain. Two

retailers only sent one message past the 10-day deadline and then stopped on their own. Two retailers stopped immediately after a second unsubscribe, but the remaining three continue to send unabated.

Though the 4% failure to honor unsubscribe requests is an improvement over 2016 it is still well above the 2% seen in 2014 and reinforces the need for retailers to continually monitor unsubscribe processes and use of suppression lists to ensure accuracy and ensure that every request is honored. In addition to facing regulatory fines, companies who repeatedly fail to honor unsubscribe requests may find themselves on "black lists" which are broadly used by ISPs and receiving networks to help identify and block abusers and spammers.

For the first time, presence of a physical address in the email (as required by CAN-SPAM) was tracked. Both street addresses and P.O. boxes were given credit, though OTA recommends use of a street address. Three retailers did not have an address, disqualifying them from "Best of Class" consideration. This is a basic requirement that can be easily corrected.

EMAIL INDUSTRY LEADERS

The 2017 Audit includes a "Best of Class" designation for retailers which scored 80% or better and were CAN-SPAM/CASL compliant. As shown in Figure 19, of retailers who sent newsletters / promotional messages, 67.4% achieved this distinction, a slight decline from 2016.

Reasons for the decline in Best of Class achievement from 2016 vary, but the major factors were retailers with no physical address in the email, retailers who failed to honor the unsubscribe request and the new criterion requiring sessions to unsubscribe pages to be encrypted.

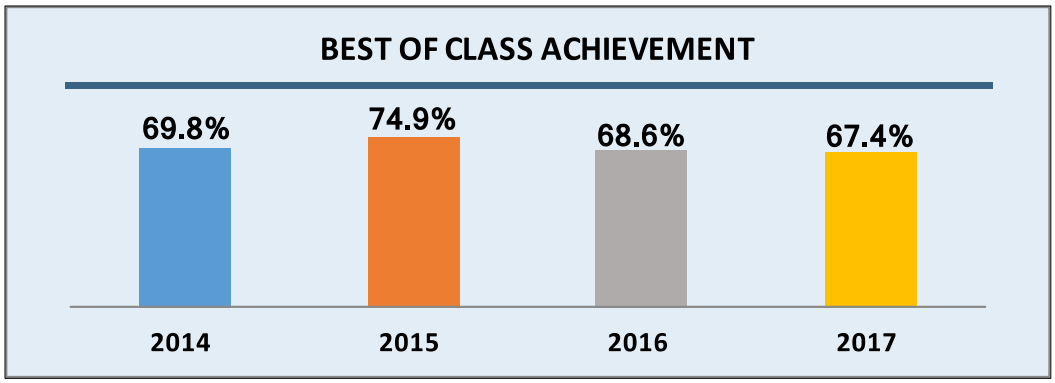


Figure 19 – Best of Class Achievement, 2014-2017

The number of perfect unsubscribe scores (adopted all twelve best practices, did not send an unsubscribe confirmation email and did not violate CAN-SPAM / CASL) dropped from 23 in 2015 to 12 in 2016 to 9 this year. The retailers receiving perfect scores in 2017 were: BlueNile.com, HSN.com, LandsEnd.com, MusiciansFriend.com, SierraTradingPost.com, StitchFix.com, Talbots.com, ToysRUs.com and Walgreens.com.

Five retailers repeated their perfect scores of 2016: BlueNile.com, HSN.com, LandsEnd.com, SierraTradingPost.com and Walgreens.com. A complete list of retailers who earned both perfect scores and Best of Class status, including the number of consecutive years they have qualified, can be found in the Appendix on page 30.

This year analysts also looked at retailers who had full adoption of email authentication and security, as defined by supporting all of the following in their newsletter/promotional emails – SPF, DKIM, DMARC enforcement (a policy of reject or quarantine) and Opportunistic TLS. Overall, 29% had this full adoption, and 35 of the "Best of Class" recipients were in this category. The Appendix on page 30 has a "**^**" next to each retailer who had full email authentication and security adoption. OTA recognizes that this does not necessarily indicate those same retailers have similar adoption on their corporate email or other email subdomains.

METHODOLOGY & LIMITATIONS

OTA's Email Marketing & Unsubscribe Audit focused on the top 200 North American e-commerce sites based on revenue as of December 2016, as reported by Internet Retailer Magazine. In total, 25 sites on the list changed from 2016 to 2017. Most of this was due to changes in ranking from year-to-year, consolidation and acquisitions. The remainder was tied to OTA analysts' ability to qualify for sign up on certain sites (e.g., required specific geographic location, certain membership qualifications or up-front payment for account creation/subscription). To maintain the integrity of the sample size, OTA continued down the list (to the 210th ranked retailer) until a total of 200 subscriptions were made.

Initial signups utilized a Gmail address and were completed the week of March 20, 2017 as part of the data gathering for OTA's annual Online Trust Audit. Additional subscription requests were made in mid-May and mid-August for retailers who had not responded, had only sent a confirmation with no follow up, or who had stopped sending. Unsubscribe requests commenced in mid-August and were tracked through the end of September. If necessary, additional unsubscribe requests were issued during September.

Based on a public comment process, including interviews with leading email service providers, regulators and stakeholders, scoring criteria were refined this year, generally resulting in more rigorous scoring. Two new criteria were added – examining whether the unsubscribe address was auto-populated during the unsubscribe process (especially important for users who consolidate multiple email addresses in one inbox) and whether sessions to the unsubscribe pages were encrypted (prevents transmission of sensitive information in the clear).

As in the last two years, the criteria were weighted in two layers – higher weight was given to "core" best practices, less weight was given to "advanced" best practices and a penalty was assigned to companies who sent an unsubscribe confirmation email. A total of 100 points were possible and violation of CAN-SPAM / CASL (including lack of presence of a physical address in the email) caused automatic disqualification from Best of Class consideration.

Testing was completed using Microsoft Windows PCs running Windows 10, Chrome and Gmail and MacBooks running macOS Sierra, Chrome and Gmail. Web pages were examined at a "Zoom" setting of 100%, primarily using Google Chrome, though some were examined using Microsoft Edge. While this Audit did not specifically test email rendering on mobile devices, the importance of mobile testing is critical considering both the popularity of reading mail and the reduced display size and usability limitations. Additional tools (FontFace Ninja and Color Contrast checker, both Chrome add-ins) were used this year to accurately measure the font size and contrast ratio of the unsubscribe text.

OTA recognizes that organizations' audited marketing practices, processes and service providers may have since been modified or changed. It is important to note that some of the best practices outlined may not be applicable for organizations of every sector or size.

It is likely that future reports will be expanded to assess the practices of retailers outside North America.

SUMMARY

Email marketing continues to grow and is a preferred channel for most companies because it provides a way to engage users directly and personally with relevant content. Still, many users experience "email fatigue" with overloaded inboxes, and in light of business email compromise and other phishing attacks, there is increasing concern about the validity of email in the inbox. Combined with tightening regulations such as GDPR, email marketers need to be as diligent as ever about their practices.

Marketers can maximize consumer engagement, clear regulatory hurdles and maximize protection for both their subscribers and their brand by: sending relevant messages at a pace selected by the consumer; allowing them a high degree of choice and control; setting expectations though transparent disclosure about use of data and consequences of choices; and protecting the integrity of email and websites through use of email authentication and encrypted email transfers and web sessions.

The results of the 2017 analysis confirm that the vast majority of top online retailers follow best practices beyond mere compliance. Though the number of retailers achieving "Best of Class" status and perfect stores declined slightly from 2016, mainly due to newly introduced criteria and tightening of other criteria, overall adoption of scored best practices grew in nearly every category, including email authentication.

However, there are areas of concern – the streamlining of signups and the continued decline in discoverability of the unsubscribe link. Though minimizing signup friction is understandable, given regulatory shifts (especially GDPR) companies need to consider collecting more data upon signup (especially data related to citizenship and residency) and set clear expectations about use of the data collected and consequences of consumers' choices. Regarding the discoverability of the unsubscribe link, there seems to be a divergence in approach, with the best getting better and the rest obscuring the link even more. OTA encourages all marketers to make the unsubscribe link highly discoverable and examine the best practices of their peers.

Overall, OTA commends marketers and email service providers (many of whom contributed to the criteria and content of this report) for their commitment to consumer empowerment and control of their inbox. As with other areas researched by OTA, maximizing trust is not a one-time event – it requires diligence and continual monitoring of marketing and subscription practices to ensure ongoing conformity to best practices and regulatory changes.

Failure to monitor these processes risks regulatory oversight, suboptimal inbox placement or blocking by mailbox providers, consumer frustration and lost business. With the EU's GDPR deadlines fast approaching, all companies need to re-evaluate their marketing, privacy and security practices.

We have a shared responsibility to improve the integrity of the email channel, taking into account feedback from consumer advocacy groups, marketers, ESPs and mailbox providers. OTA has been encouraged by the ongoing input and collaboration of organizations across the spectrum to help promote and refine these best practices. As marketers give consumers more choice, notice and control, trust will increase, enabling the email and marketing industry to continue to thrive.

Updates to this report and resources are posted at https://otalliance.org/unsub. To submit comments or suggestions, please email admin@otalliance.org.

RESOURCES

REGULATORY

Australian Communications and Media Authority (ACMA)

http://www.acma.gov.au/Home/Industry/Marketers/Anti%20Spam

Mandatory Unsubscribe Facility
http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/mandatory-unsubscribe-ability-ensuring-you-dont-spam-i-acma

Canada's Anti-Spam Legislation (CASL)

FAQ's – http://www.crtc.gc.ca/eng/com500/faq500.htm

EU General Data Protection Regulation (GDPR) – Goes into effect May 25, 2018

Home page https://www.eugdpr.org/, Neatly arranged https://gdpr-info.eu/

New Zealand – Department of Internal Affairs – Anti-Spam Guidelines
http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Spam-Index?OpenDocument

United Kingdom – Information Commissioner's Office Electronic Mail Marketing & The Privacy and Electronic Communications Regulations (PECR)
https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/electronic-mail-marketing/

U.S. Federal Trade Commission

CAN-SPAM Act: A Compliance Guide for Business
http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business

Complying with the CAN-SPAM Act (Video)
https://www.ftc.gov/news-events/audio-video/video/complying-can-spam-act

INDUSTRY BEST PRACTICES

Unsubscribe Resources & Report Updates – https://otalliance.org/Unsub

OTA Marketing & Integrity – https://otalliance.org/Emailintegrity

OTA Email Authentication – https://otalliance.org/eauth

Online Trust Audit – https://otalliance.org/TrustAudit

Site Encryption – https://otalliance.org/AOSSL

ACKNOWLEDGEMENTS

The research paper is a collaborative work product reflecting input from industry leaders and government agencies worldwide. Industry input has been provided by Act-On Software, Agari, AgeLight, American Greetings, Basegrow, Epsilon, Constant Contact, Harland Clarke Digital, Dmarcian, LashBack, Iconix, Marketo, Microsoft, OPTIZMO, Publishers Clearing House, Relevancy Group, Symantec, UnsubCentral, ValiMail and Yes Lifecycle Marketing. In addition, special thanks to lead researcher Jeff Wilbur, editor Craig Spiezle and Ryan Polk, Steve Olshansky, Christine Runnegar and Madelon Smith for their contributions.

ABOUT THE ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance is an initiative within the Internet Society. OTA's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, ethical privacy practices and data stewardship.

The Internet Society is a non-profit organization dedicated to ensuring the open development, evolution and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that enable universal access. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

To learn more visit https://otalliance.org.

APPENDIX – 2017 BEST OF CLASS

4 1800Flowers.com
3 1800PetMeds.com
2 adidas.com
2 AdvanceAutoParts.com
4 AE.com
2 Aeropostale.com
AlliedElec.com
4 AmericanGirl.com/shop
AnnTaylor.com
4 Art.com ^
2 ASOS.com ^
AutoPartsWarehouse.com ^
2 AutoZone.com ^
4 Avon.com
Backcountry.com
4 BassPro.com
3 BedBathandBeyond.com
4 Belk.com
4 BestBuy.com
BlueApron.com
4 **BlueNile.com ^**
2 BN.com
BodenUSA.com
4 BonTon.com ^
3 BrooksBrothers.com
2 Build.com ^
3 BuildDirect.com
Cabelas.com
CalvinKlein.com
4 Carters.com
4 ChildrensPlace.com ^
Coastal.com
2 Columbia.com
4 Costco.com
4 CrateandBarrel.com
2 Crutchfield.com
2 CVS.com
2 Cymax.com
Dell.com
DSW.com ^
2 DuluthTrading.com
4 EddieBauer.com
3 EdibleArrangements.com ^
EsteeLauder.com
4 Etsy.com ^
3 Evine.com
4 Fanatics.com
Fingerhut.com ^
2 FocusCamera.com
4 FootLocker.com
2 Fossil.com ^
GameStop.com ^
4 Gap.com ^
Gemvara.com ^
3 Groupon.com ^
HomeDepot.com
3 Honest.com
HP.com
4 **HSN.com**
Ikea.com
JamesAllen.com
4 JCrew.com ^
JMBullion.com
3 Jomashop.com ^
4 JPCycles.com
2 JustFab.com
4 Karmaloop.com
4 Kay.com ^
3 Keurig.com
Kohls.com
2 Kroger.com
2 Lakeside.com
3 **LandsEnd.com**
3 Lenovo.com ^
2 Levi.com ^
3 Lowes.com
4 LuluLemon.com ^
4 Macys.com ^
2 MensWearhouse.com
2 MLB.com
MSCDirect.com
2 **MusiciansFriend.com**
3 Newegg.com ^
4 NFLShop.com
4 Nike.com
4 Nordstrom.com ^
4 NorthernTool.com
3 Nutrisystem.com ^
4 OfficeDepot.com
4 OpticsPlanet.com
4 OrientalTrading.com
4 Orvis.com
4 Overstock.com ^
Patagonia.com
Peapod.com
Petco.com
Pier1.com ^
2 PotpourriGift.com
3 Puritan.com
4 REI.com ^
RestorationHardware.com ^
3 RevolveClothing.com
Rubbermaid.com
3 Safeway.com
3 Sears.com
3 SearsOutlet.com
Sephora.com
shoebuy.com
2 ShoeMall.com
Shop.com
Shutterfly.com ^
4 **SierraTradingPost.com**
StitchFix.com ^
4 Sweetwater.com
SwissColony.com
4 **Talbots.com**
4 TheBay.com
TheRealReal.com
4 TheShoppingChannel.com
4 TireRack.com
4 ToryBurch.com
2 **ToysRUs.com ^**
UGGAustralia.com ^
3 ULTA.com
4 UnderArmour.com
4 VictoriasSecret.com
3 Vistaprint.com
4 **Walgreens.com**
3 WBMason.com
3 WeightWatchers.com

2 3 4 – Number of consecutive years as Best of Class **Bold** = Perfect Unsubscribe Score

^ – Supports all of the following for the email marketing domain: SPF, DKIM, DMARC enforcement and Opportunistic TLS

Rev1206