Online Trust Alliance

2016 Email Marketing & Unsubscribe Audit

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

Released November 2, 2016

TABLE OF CONTENTS

BACKGROUND

As a global non-profit, the mission of the Online Trust Alliance (OTA) is to enhance online trust and empower users, while promoting innovation and the vitality of online services. Through fostering collaboration and convening a public-private dialog, OTA develops best practices focused on enhancing user trust, data security and responsible privacy and marketing practices. 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.

Identifying best practices to help bolster the integrity of the email marketing channel is one of OTA's key initiatives. By all accounts, email marketing is an affordable and effective way to reach customers, maintain loyalty, inspire purchases and establish positive consumer brand perception. With over 4.4 billion email accounts in use today, email marketing continues to outperform display and search advertising.[1]

While growth of the channel is encouraging, many consumers are facing email fatigue, finding email not relevant, thereby driving the loss of subscribers.[2] Consumers are more sensitive than ever, often marking legitimate messages as spam, perceiving them to be irrelevant or arriving too frequently.

In a continuing series of benchmark reports, OTA has initiated the 3rd Annual Email Marketing Audit, assessing the end-to-end user experience from sign up through the 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. The overarching goal is to enhance the brand experience and build trustworthy consumer engagement.

Working through a multi stakeholder effort, 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. With a goal to enhance the user experience and fight abuse, the criteria and scoring are re-evaluated annually to address trends, best practices and international regulatory compliance requirements. Leveraging learnings from the annual Online Trust Audit[3] and the 2016 Native Advertising Transparency report,[4] the bar was raised this year to reflect current best practices.

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 practices outlined 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] Radicati Group Inc. http://www.radicati.com/
[2] FirstInsight Retail Email Overload http://cdn2.hubspot.net/hubfs/160569/retail_email_overload_2-8-16.pdf?t=1461241656465
[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 2016 Audit found that the vast majority of top online retailers have embraced unsubscribe best practices that go beyond mere compliance and have shown improvement since 2014 despite more stringent criteria. This year's audit was expanded to examine the entire email engagement process, from signup to the unsubscribe user experience. Consistent with the 2015 and 2014 reports, the Audit focused on the top 200 online retailers.[5] For each site, analysts measured and tracked the sign up process, and after observing emails received for over a month, each account was unsubscribed, and activity and compliance was monitored for a period of 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. Marketers achieving scores of 80% or higher received designation as "Best of Class." For 2016, 69% of the top retailers qualified, a drop from 75% in 2015 and roughly equal to 2014. Twelve sites had perfect scores – Blue Nile, Carter's, CDW, Evine, HSN, Jomashop, Lands' End, Sierra Trading Post, Sweetwater, ULTA, Walgreens and Wayfair.

In spite of these improvements, the average scores decreased in 2016, raising a call for self-examination by the online marketing community to put the user first and embrace the outlined practices. The results will provide dividends in engagement, deliverability and brand reputation. As the regulatory landscape is evolving, marketers need to look beyond North America to the General Data Protection Regulation (GDPR), which carries potential fines of up to 4% of global revenues for violation of marketing, privacy and data protection practices.[6]

"The user experience is essential to building trust in the email channel and the brands consumers interact with. It is paramount to put the user first by giving them control through the use of preference centers, transparent privacy policies and one-click unsubscribing."
Michael Fisher, President
Yes Lifecycle Marketing

KEY FINDINGS

Overall Results

- 68.6% of sites qualified as "Best of Class," scoring 80% or higher and being CAN-SPAM / CASL compliant, down from 2015
- 12 sites had perfect scores (a significant drop from 23 last year). Primary causes for this decline include: 1) sites no longer soliciting customer feedback, 2) sites no longer offering a preference center or opt-down choices and/or 3) failure to render a "clear and conspicuous" unsubscribe link

Signup Practices

- 6% of sites used Confirmed Opt-In (COI) to verify subscriptions, down from 11% in 2015
- Only 3% of sites used CAPTCHA to reduce the risk of bot signups and "list bombing"

[5] Source: Internet Retailer® https://www.internetretailer.com/top500/
[6] GDPR Overview http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Mailing Practices

- Use of email authentication to fight spoofed and malicious email was exceptional, with 94% supporting SPF, 98% supporting DKIM and 51% supporting DMARC
- Use of the unsubscribe header (which presents as a link or button in many consumer client mailboxes) increased by four points over last year to 89%

Unsubscribe Practices

- Use of "clear and conspicuous" unsubscribe links was 81%, declining significantly from 97%
- Use of adequately-sized text dropped to 93% from 98%
- Use of commonly understood terms (disclosure) dropped to 89% from 94%
- Use of branded confirmation pages rose slightly to 93% from 90%
- Use of preference centers decreased significantly to 38% from 56%
- Offer of opt-down (reducing the mailing frequency) decreased to 33% from 45%
- Only 23% of sites asked for customer unsubscribe feedback, essentially unchanged from last year

Unsubscribe Results

- 86% stopped sending messages immediately after the unsubscribe request (versus waiting the permitted 10 days), an improvement from 83% in 2015
- Total violations of CAN-SPAM / CASL were 5.9% (11 retailers), down from 7.1% (13 retailers) last year
    - Eleven mailed 10 days past the unsubscribe request, nearly a four-fold increase from 2015
    - None had a broken unsubscribe link, a significant improvement from 10 retailers in 2015

OBSERVATIONS

Signup Practices

The 2016 Audit analyzed the entire signup process for the first time, including the risk of fraudulent newsletter subscriptions being sent by third parties. This addition was in response to several recent high-impact incidents where cybercriminals deployed bots and other mechanisms to sign up targeted email addresses to thousands of email lists. Known as "list bombing," users including media and government officials found their inboxes flooded with up to ten thousand "subscriptions," rendering the accounts useless.[7] Not only impacting consumers, many marketers found their domains blocked by the anti-spam community, further compromising their brand integrity while their systems were unknowingly exploited.

In response, OTA expanded the Audit to evaluate the presence of processes used to help curb this abuse, focusing on anti-bot mechanisms and confirmed opt-in (COI). Unfortunately only 3% required the completion of a CAPTCHA to help prevent bot signups.[8] Additionally, only 6% utilized COI, requiring the consumer to click a link to confirm the subscription was requested.[9] The COI adoption rate is especially concerning as it declined from 11% in 2015 even though abuse levels have increased. Marketers have reported that the decrease is due to difficulty with the process – when users inadvertently or mistakenly do not confirm (including the challenge

[7] https://krebsonsecurity.com/2016/08/massive-email-bombs-target-gov-addresses/
[8] Subscription Bombing, ESPs and Spamhaus https://wordtothewise.com/2016/08/subscription-bombing-esps-spamhaus/
[9] CAPTCHA, "Completely Automated Public Turing test to tell Computers and Humans Apart" https://en.wikipedia.org/wiki/CAPTCHA

to confirm if the message lands in "clutter" or "junk" where links are disabled), it can frustrate consumers and impact subscription goals. At the same time, the lack of use of CAPTCHA and COI leaves retailers open to abuse and can reduce net engagement rate. Future audits may integrate these practices into the scoring.

OTA analysis showed that 34% of top retailers pop up a screen to invite signups on the consumer's first visit, 31% make a promotional offer via the web site upon signup and 89% confirm the signup on the site. In the data entry area, 16% require double entry of the email address to reduce errors, 41% request additional information (e.g., name, address, preferences) and 20% require an account to be created.

Mailing Practices

The list of practices monitored was expanded to include more rigorous analysis of welcome/confirmation messages (and associated promotional offers), mailing cadence over time, and use of email authentication for newsletters/promotional messages.

"Email is a vibrant and effective mechanism to build a brand and drive results, but it must be built on a subscription and unsubscribe process which are user-centric: built on preferences and respect," Sal Tripi, AVP Publishers Clearing House.

Of the 200 online retailers assessed, 79.5% sent confirmation and newsletters/promotional messages, 14.5% sent only newsletters/promotional messages, 4.0% sent only a confirmation and 2% never responded. 46% of the confirmation messages contained a promotional offer (e.g., free shipping, discounted orders).

As expected, the cadence of messages varied widely, likely due to varying business models of the retailers. Sites promoting daily deals sent as many as three messages per day, while some sites sent newsletters just once a month. The research revealed some interesting approaches – some retailers automatically reduced the cadence over time (e.g., from every other day to twice a week to twice a month) as they detected non-engagement from the OTA test account, and many (28%) proactively stopped sending altogether after a period of non-engagement.

Email authentication has become a fundamental requirement to both optimize inbox delivery and help counter spoofed and malicious email purporting to come from legitimate brands. Audit results showed that the use of email authentication for the domains used to send newsletters/promotional messages is exceptional – 94% supported SPF, 98% supported DKIM and 51% supported DMARC.[10] Additionally, 50% of the retailers with DMARC records have made policy assertions of "reject" or "quarantine," effectively telling recipients to block or sideline messages that fail authentication. This level of DMARC adoption is relatively low, but it is growing as more retailers are taking steps towards protecting the integrity of the email channel.

The following sections provide a detailed examination and analysis of the unsubscribe process and consumer experience including focus on disclosure, discoverability and delineation of the unsubscribe link.

[10] Email Authentication Protocols & Best Practices https://otalliance.org/eauth

SIGNUP PRACTICES

In the 2016 Audit, signup practices were tracked and analyzed in greater detail. This added focus on the practices deployed is to create a baseline for future studies and scoring models. The analysis included any proactive efforts or incentives to recruit registrations, the data required for subscription and steps to validate the subscriber's address. The results are shown in Figure 1 below.

SIGNUP PRACTICES	
Invitation	
Pop-Up Invitation to Subscribe to Email	34%
Promo Offer on Screen for Signing Up	31%
Signup Confirmation on Screen	89%
Data Entry	
Required Email Address to be Entered Twice	16%
Requested Additional Information	41%
Required Account Creation	20%

Figure 1 - Signup Practices

INITIAL INVITATION/ENGAGEMENT

The testing process entailed visiting each retailer's website intending to subscribe to newsletters/promotions. Sites were evaluated on the discoverability and ease of signup and any signup incentives. As shown in the example in Figure 2, 34% of retailers encourage signup through homepage overlays or pop-over windows. Most have a signup box or link on the home page, typically either in the upper (header) area or the lower (footer) area of the page. While not measured, several sites made efforts to maximize registrations by including multiple registration links – on the header, within menu navigation and in footer of the page.

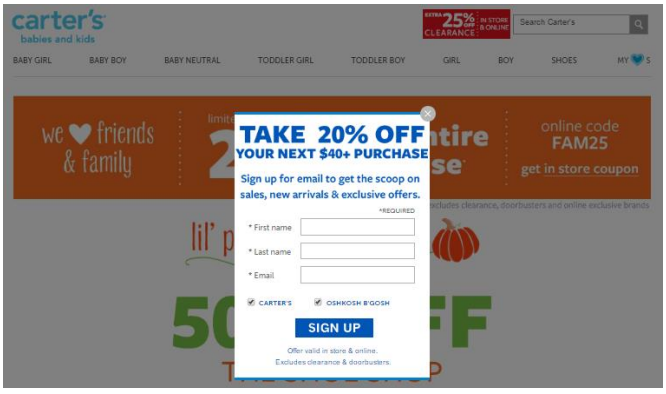

Figure 2 - Example of Pop-Up Window Inviting Subscription

Further engagement was made by offering a promotion of some kind (e.g., free shipping, discount on first order) when subscribing. Incentives were offered by 31% of the sites – 70% of these sites also made an offer via a welcome email, while 30% did not. Not reiterating an offer or promo code could be a lost opportunity to engage the customer and may even cause customer confusion. Finally, 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 89% of retailers.

DATA ENTRY

Requiring an email is all that is necessary to initiate a subscription, but there are 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 their needs and 3) to help maximize regulatory compliance, knowing the state/province and country one resides in.

OTA observed that 16% of retailers required the email address to be re-entered, 41% requested additional information about the subscriber, and 20% required account setup (this requirement clearly varies by business model). OTA recommends requiring a user to enter the address twice to reduce the risk of users mistakenly typing in a wrong address. Some systems use a real-time verification or real-time hygiene solution to address this issue.

As a best practice OTA advocates the prompting of additional information over time, with the goal of enhancing profiling capabilities. 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 the cadence or frequency aligned with their expectations.

SUBSCRIBER VALIDATION

Unauthorized and fraudulent email subscription abuse has dramatically increased over the past year. Users have been targeted and "list bombed," causing them to receive hundreds of unsolicited emails within minutes. Unknowingly, email marketers and their service providers' infrastructures have been compromised, effectively incapacitating users' email accounts. While the signup process is fast and efficient for users, this ease of use has been exploited by automated signup bots. As a result, mailers have found their domains and IP addresses blocked by Spamhaus and others, while targeted users had to individually unsubscribe from each email.[11] To help address this risk OTA recommends that sites consider two simple practices.

The use of CAPTCHA (as shown in Figure 3) can help to verify that the subscriber is a real person and not a bot. While this doesn't prevent bogus subscriptions, it does reduce their scale since they can't be easily automated. Likewise, 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 this does not prevent list bombing, it does prevent users from receiving multiple emails or having to unsubscribe. They can simply ignore it, discard the email or block the sender. While COI can significantly reduce signup abuse, it

[11] Spamhaus an international nonprofit that tracks spam and related cyber threats, providing threat intelligence to the Internet's major networks, corporations and security vendors, to identify and pursue spam sources. https://www.spamhaus.org/

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 low.

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 two years, but this is the first year to examine the use of CAPTCHA during the signup process. As noted in Figure 4, 3% of retailers use CAPTCHA to prevent bot signups, while 6% of retailers use COI during the subscription process. Use of COI dropped by nearly half since 2015 (11%), which is a concern – 8 sites that utilized COI in 2015 no longer do, raising the risk of abuse. As a best practice to limit abuse, 5 retailers utilize both CAPTCHA and COI during the signup process.

While such practices add sign-up friction, they also add value – to make a brand's site less attractive for abuse, help protect users' inboxes, and protect the brand's reputation, ultimately increasing user trust and engagement in the process. 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
Confirmed Opt-In (COI)	7.9%	13.1%	6.0%
CAPTCHA	-	-	3.0%

Figure 4 - Subscription Validation Practices, 2014-2016

MAILING PRACTICES

Building upon the 2015 methodology, additional elements 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 for newsletters/promotional messages and the mailing "cadence" or frequency of mailing.

SUBSCRIPTION RESULTS

As shown in Figure 5, this year nearly 80% percent of marketers demonstrated the best practice of sending a signup confirmation and subsequent newsletter, on par with 2015 results. Nearly 15% skipped the welcome message and moved directly to newsletters/promotions. Of concern is a total of 6% that either never sent any response or sent only a confirmation with no subsequent newsletters or offers. While this is an improvement over 2015 (8.5%), it reflects a lost revenue opportunity. In instances where no confirmations or newsletters/promotions were received, a second subscription using a different email address was completed. In most cases this solved the problem, but as outlined, even after 90 days, 4 retailers never sent any emails, a slight improvement over 2015 results.

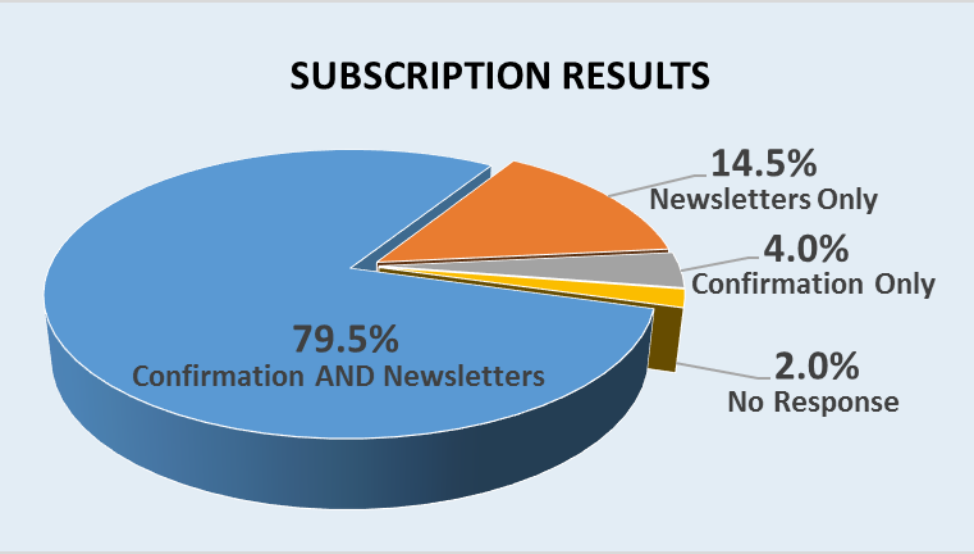

Figure 5 - Subscription Results, 2016

EMAIL AUTHENTICATION

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. Leading global email authentication standards include Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). When deployed together they help ISPs and corporate mail systems (receivers) detect and prevent email spoofing while enhancing deliverability of legitimate messages. Domain-based Message Authentication, Reporting and Conformance (DMARC) enhances the capability by: 1) allowing senders to specify a policy to receivers if messages fail authentication and 2) receiving abuse 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 and others.

Building on the annual Online Trust Audit, a rigorous analysis of email authentication in retailers' newsletters/promotions was conducted. As outlined in Figure 6 the results are very positive. Authentication of newsletter domains is significantly higher than the same retailers' top-level (corporate) domains. Though it is surprising that DKIM support exceeds SPF support by a few points (in general SPF is more widely adopted than DKIM), these adoption rates are excellent. Most important is the high rate of adoption of DMARC policy assertions which instruct receivers to quarantine or reject email that fails authentication.

EMAIL AUTHENTICATION

	Newsletter Domains	Top-Level Domains	Delta
SPF	94.1%	82.5%	*+11.6%*
DKIM	97.9%	37.0%	*+60.9%*
DMARC Record	50.5%	27.3%	*+23.2%*
% with Quarantine Policy	6.3%	0.0%	*+6.3%*
% with Reject Policy	43.2%	4.5%	*+38.7%*
Use of Opportunistic TLS	31.9%	73.3%	*-41.4%*

Figure 6 - Email Authentication - Newsletter Domains vs Top-Level Domains, 2016

These practices are becoming increasingly important for marketers. Email authentication helps ISPs and mailbox providers properly assess messages and can improve deliverability. The surprise is the low rate of TLS adoption by newsletter domains (32% vs 73% at the TLD), which is likely tied to the use of TLS by email service providers. Considering the push by ISPs and mailbox providers, the lack of TLS (along with comprehensive email authentication) can negatively impact verification processes. Although TLS may not directly impact whether or not a marketer will land in the inbox, its helps mailbox providers to verify and identify senders.

Though "under the covers" and not visible to users, the absence or failure of TLS can trigger inbox display warnings, negatively impacting the user experience, open rates and user engagement.

As shown in Figure 7 below, Microsoft Outlook (green shield) and Google's Gmail (gold key) both provide users indicators when messages are authenticated properly.

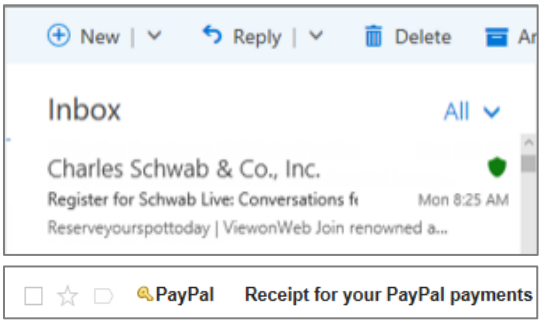

Figure 7 - Examples of Authentication Indicators in Outlook and Gmail

In February of this year Gmail started showing an unlocked red padlock (see Figure 8 below) when messages are sent without TLS.

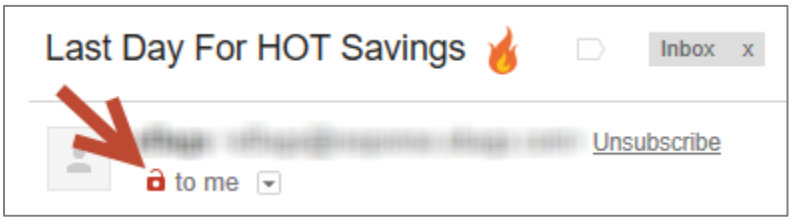

Figure 8 - Example of Gmail TLS Indicator

MAILING CADENCE

New to the 2016 Audit, the cadence of mailings, as defined by the frequency and continuation of sending email, was tracked. This data revealed interesting observations and possible enhancements for future research to test both engaged and unengaged signups for variances. 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. Given today's tools and engagement analysis, marketers may have throttled back the cadence of email received.

"List recruitment, engagement and relevancy are fundamental. A brand's ability to recognize the importance of the consumer experience can be the difference between success and failure," David Daniels, CEO the Relevancy Group

Most retailers (90%) mailed with a consistent cadence, which varied from several messages per day to once a month. However, some (18) backed off their cadence over time, likely in response to the non-engagement. In one case a retailer started with daily messages, but then backed off to one per week after 45 days. Another sent messages every three days for two weeks, then backed off to once a month. In addition, 28% of retailers actually stopped sending (without an unsubscribe) after a period of time, which varied from 4 days to 120 days, averaging about 50 days.

UNSUBSCRIBE PRACTICES

The unsubcribe process and associated user experience have represented the core analysis and reporting for the last two years. In conjunction with the email marketing community and consumer advocates, OTA has developed the list of scored best practices that maximizes user choice and control over the unsubscribe process. The criteria and description of the ten scored practices are shown 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.

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. **Readability.** The unsubscribe text should both discoverable and be 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 8 point font, 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 font family than the body copy.

   Historically email and websites have had white backgrounds, but many have switched to light greys or blues for their type. Black text on a white background has a contrast ratio of 21:1 – the maximum which can be achieved. For reference the best practice for type is a minimum contrast ratio of 7:1 so that the visually-impaired can still see text.[12] 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.

[12] Internet is becoming unreadable because of a trend towards lighter, thinner fonts http://www.telegraph.co.uk/science/2016/10/23/internet-is-becoming-unreadable-because-of-a-trend-towards-light/

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.[13] 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. 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 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. **Preference Center and/or Opt-Down.** A link should be offered directing users to a preference center to unsubscribe, opt-down or make other changes. Don't obfuscate the unsubscribe language or process. If a web-based page is used for suppression collection, consider offering options besides complete opt-out. However, do not require a user to log in with a password to change preferences, and be sure one of the preferences is a global opt-out. Consumers can also be presented with an opt-down option, giving them 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) and how often to receive them – daily, weekly, bi-monthly or monthly. Consumers want to maintain a relationship with companies' brands, but maybe not all at the same frequency. Note it is recognized that small companies and low frequency senders may not have the scale or size to offer such options.
9. **Optional Customer Feedback.** A simple survey 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 to the right of the opt-out option or on the confirmation page, but never send a follow up email asking why they unsubscribed. Allowing the customer to check off individual elements 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).

[13] IEFTC 2369 published July 1998 https://tools.ietf.org/html/rfc2369

10. **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.

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. 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 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 IoT Trust Framework.[14]

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. Knowing which state and country a user resides in will pay dividends in complying with appropriate 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.[15]
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.

[14] IoT Trust Framework – https://otalliance.org/IoT

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

8. **The unsubscribed address should be automatically populated** during the unsubscribe process to prevent typos or errors that could occur when users consolidate multiple email addresses into a single inbox. The email address of the default inbox may not be the same as the address used to subscribe, rendering a reply to the send as ineffective as the reply email address is not the same as the address on file and used by the marketer.

DISCLOSURE, DISCOVERABILITY & DELINEATION

Adoption of best practices in the email decreased in all but one category, somewhat due to more rigorous application of the criteria, but also due to a "softening" of the discoverability and delineations of the unsubscribe link. In many cases retailers obfuscated or buried the link in lines of text, reduced contrast or visibility of the link, or combined it with other choices (e.g., "if you'd like to stop receiving our emails or modify your email preferences, click here").

AUDITED & SCORED BEST PRACTICES IN THE MESSAGE

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

Figure 9 - Adoption of Scored Criteria in the Message, 2014-2016

As shown in Figure 9, "Clear and Conspicuous" display of the unsubscribe link decreased from 97% to 81%, representing the largest change of any criteria. The "Easily Read / Size" and "Commonly Understood Terms" criteria also dropped, though less dramatically. Some examples are shown below in which retailers are blurring the lines in these areas by hiding the link or using fuzzy language.

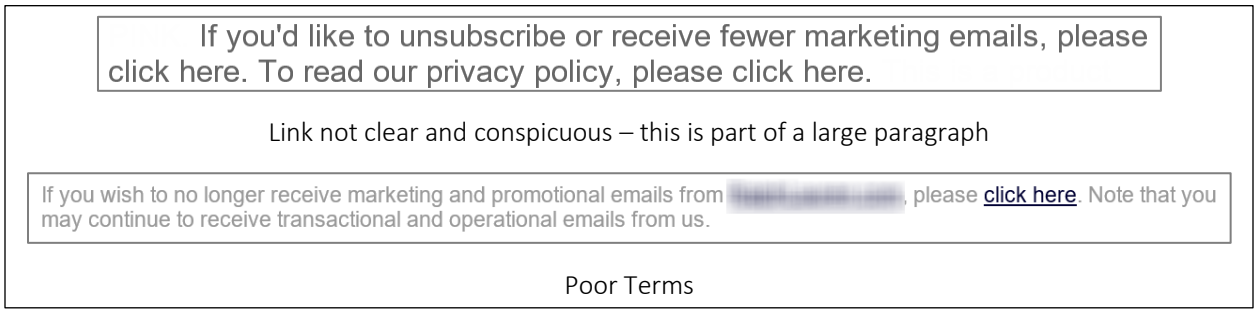

Figure 10 - Examples of Poor Disclosure, Discoverability and Delineation

The one bright spot was adoption of the unsubscribe header, which continues to grow, from 76% in 2014 to 89% this year. Given the emphasis on safe and discoverable unsubscribe mechanisms, it is important for marketers to understand that most consumer mailboxes will render this option when the unsubscribe header is included in the email.

Figure 11 - Example of Unsubscribe Header Presentation in Gmail

UNSUBSCRIBE PROCESS

The unsubscribe process was initially the core focus of this annual audit. Figure 12 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) presentation of a preference center / opt-down choice during the process and 4) 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
Opt-Out All Email	93.7%	97.3%	99.5%
Confirmation Web Page	95.2%	94.5%	98.9%
Branded Page	85.7%	90.2%	92.6%
Preference Center and/or Opt-Down	91.0%	61.7%	58.5%
Preference Center	-	55.7%	37.8%
Opt-Down	-	44.8%	33.0%
Optional Customer Feedback	24.9%	24.0%	22.9%

Figure 12 - Adoption of Scored Criteria in the Unsubscribe Process, 2014-2016 [16]

In actual experience, the unsubscribe process for the top online retailers ranged from concise one-click unsubscribes to a series of pages offering choices and soliciting feedback, and almost everything in between. Some experiences were elegant and stayed within the retailers' richly branded environment while others were raw, appearing sophomoric. In one example, upon landing on an unsubscribe page, a video ad ran before allowing a user to unsubscribe. Strong examples and counter-examples for many of the best practices are presented in the figures below.

One practice not listed in Figure 12 but which can have a significant positive impact on the user experience is the "auto-population" of the address to be unsubscribed. OTA has tracked this practice for the last two years and it remains nearly flat at 92%. Since most consumers use multiple email addresses, and many forward and consolidate multiple addresses into a single mailbox, it is often difficult for consumers to definitively know which email address they subscribed with. Auto-populating the subscribed email address (which is accessible

[16] 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.

from within the message) is convenient for consumers and reduces errors, frustration and complaints. While infrequently used for consumer email, asking a user to reply with “unsubscribe” in the subject line 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.

As shown in Figure 12, the ability to opt out of all email grew slightly and is now just shy of 100%, as is the use of a web page to confirm the unsubscribe request. Use of branded unsubscribe pages also grew modestly, from 90.2% to 92.6%. Though the rationale to use branding on the confirmation page should be obvious, some unsubscribe web pages were jarring in their simplicity, as shown in Figure 13 below.

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 an Email Service Providers (ESPs), integration can be challenging, though most ESPs offer a way to extend the corporate branding experience into the unsubscribe process.

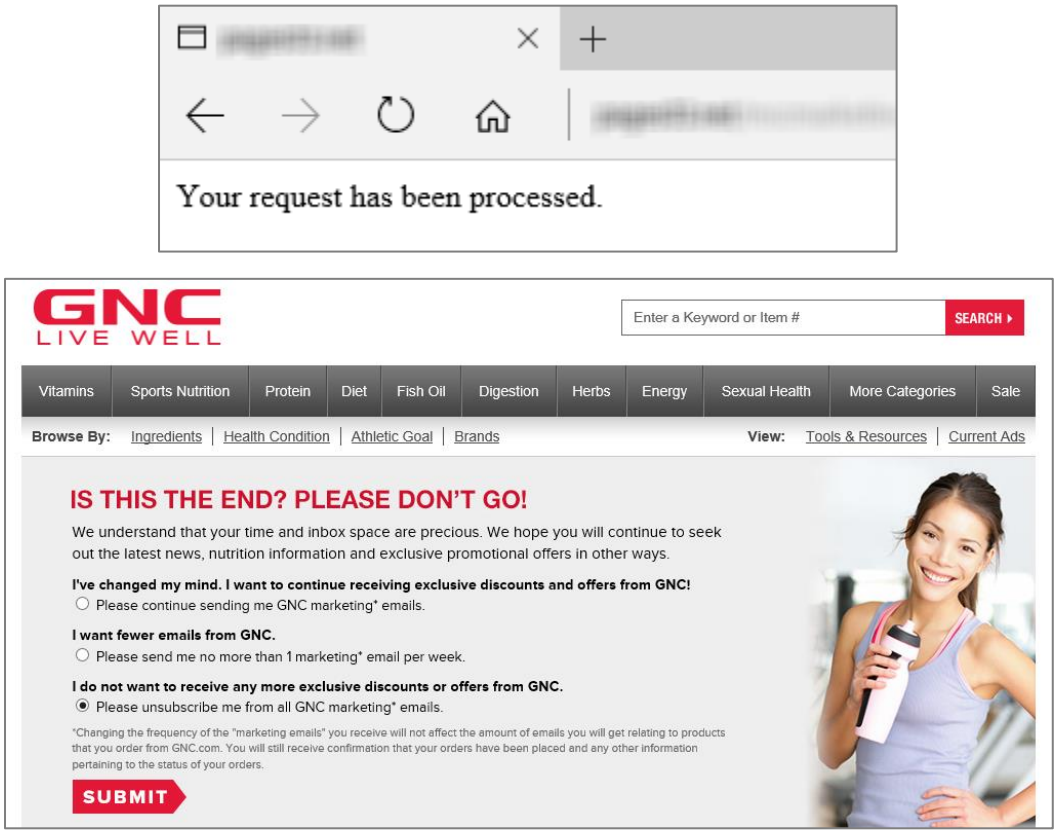

Figure 13 - Contrasting Examples of Branding in Unsubscribe Pages

The area where adoption continues to decline is the use of Preference Center / Opt-Down, which fell from 91.0% in 2014 to 61.7% in 2015 to 58.5% this year. It should be noted that in 2014, credit was given if a preference center / opt-down option was available via any path (including from within the email message itself). In 2015, retailers only earned credit for this practice if the preference center / opt-down choice(s) was offered during the unsubscribe process – this caused a dramatic drop, from 91% to 62%.

More concerning than the modest drop in combined use are the underlying specifics – use of preference centers dropped from 55.7% in 2015 to 37.8% this year. Additionally the use of opt-down options decreased from 44.8% in 2015 to 33.0% this year. This decline can be attributed to a combination of factors including changing of service providers, difficultly of managing preference centers and low user engagement of this feature. OTA encourages organizations with multiple brands and segmented offerings to embrace and support preference centers to maximize user choice and relevancy while minimizing list abandonment. It is important to note ESP capabilities and analytics across multiple marketing channels have grown significantly. Increasingly they are incorporating web tracking data making it easier to determine consumers' interests and tune their marketing activities without the need of a preference option.

In addition, rather than waiting for a user to unsubscribe, marketers should consider providing inactive subscribers a link to a preference center. Preference centers provide the opportunity to identify types of products, offers and communications they prefer. Understanding what is of interest to users is an important step to mitigating email fatigue and unsubscribe requests.

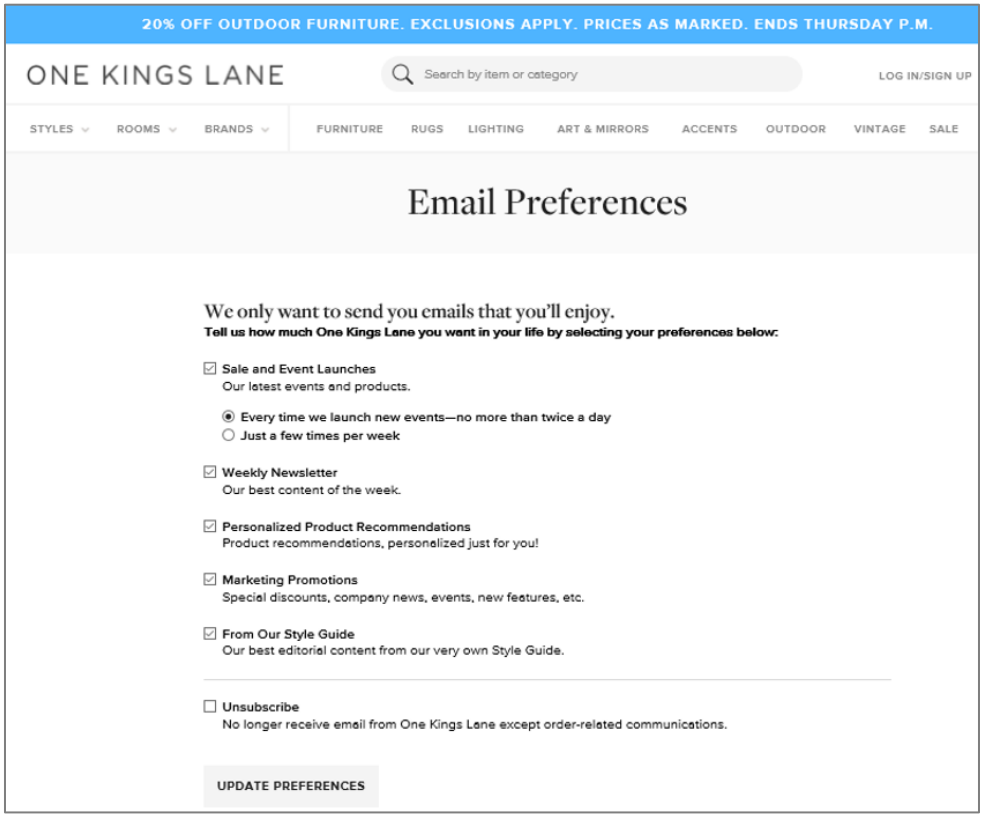

Figure 14 - Example of Preference Center / Opt-Down Choices

Figure 14 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 message take consumers to this type of page. OTA strongly encourages this approach in which users get many choices, including changing the type and frequency of emails they receive.

One of this year's disappointments is relatively low adoption of requesting optional customer feedback, which has stayed flat at 23%. A best practice is to offer the user the option of completing a brief survey or marking boxes indicating top reasons why they are unsubscribing. Note that this cannot be required to unsubscribe and must be presented after clicking the link to unsubscribe. 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.

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 or continuing to send email more than 10 business days after the unsubscribe request was submitted.

As shown in Figure 15, immediate honoring of unsubscribe requests grew to nearly 86%. This shows that the vast majority of retailers go beyond compliance to stewardship. While one-seventh of retailers have room for improvement, the vast majority recognize that sending messages after the unsubscribe request has no upside and can only annoy consumers, increasing spam complaints.

Figure 15 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
Unsubscribe Confirmation Email	4.8%	2.7%	2.7%
No Delay on Removal	82.5%	83.1%	85.6%
Violate CAN-SPAM/CASL (fail to honor or broken link)	10.9%	7.1%	5.9%
Failed to Honor Unsubscribe	-	1.6%	5.9%
Broken Unsubscribe Link	-	5.5%	0.0%

Figure 15 - Unsubscribe Results, 2014-2016

Of the five companies who issued an unsubscribe confirmation email, they all acknowledged the unsubscribe request and stated that it would be honored within a short period. Four of the five offered a link to "change

email preferences" if the recipient changed their mind or had unsubscribed in error. The fifth was 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 nearly quadrupled to 5.9% (11 retailers). Of these retailers, it appears that one changed ESPs during this time window and one appeared to be due to subscription to multiple lists (though not obvious to the subscriber). Interestingly, as seen in 2015, a few of the retailers started sending after a 30-60 day quiet period during which it seemed that they were properly honoring the unsubscribe.

Though well below the rate of 10.9% seen in 2014, this increase in unsubscribe failures is concerning 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.

EMAIL INDUSTRY LEADERS

As shown in Figure 16, of retailers who sent newsletters / promotional messages, 68.6% scored 80% or higher and were CAN-SPAM / CASL compliant. An additional 9 retailers would have qualified, but they failed to honor the unsubscribe request, sending mail more than 10 business days after the unsubscribe request, so they were automatically disqualified. Most of the violators stopped sending after a second unsubscribe request, but as of the writing of this report, two continue sending unabated.

The overall decline in "Best of Class" achievement from 74.9% in 2015 is due to a wide variety of reasons. These include: 1) lack of clear and conspicuous links and small size, 2) use of confusing nonstandard terms for unsubscribe, 3) reduced use of preference center and 4) failing to offer opt-down choices.

BEST OF CLASS

	2014	2015	2016
80% or Higher and CAN-SPAM /CASL compliant	69.8%	74.9%	68.6%

Figure 16 – Best of Class Achievement, 2014-2016

The number of perfect scores (adopted all ten best practices, did not send an unsubscribe confirmation email and did not violate CAN-SPAM / CASL) dropped from 23 in 2015 to 12 this year. Six retailers repeated their perfect scores of 2015. The retailers receiving perfect scores in 2016 are: BlueNile.com, Carters.com, CDW.com, Evine.com, HSN.com, Jomashop.com, LandsEnd.com, SierraTradingPost.com, Sweetwater.com, ULTA.com, Walgreens.com and Wayfair.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 26.

METHODOLOGY & LIMITATIONS

OTA's email Audit focused on the top 200 e-commerce sites based on revenue as of December 2015, as reported by Internet Retailer Magazine. Due to corporate consolidation and changes in ranking from year-to-year, 18 sites on the list changed between 2015 and 2016. In addition, one retailer was removed from consideration because of specific membership requirements not met by OTA analysts. To maintain the integrity of the sample size, OTA subscribed to an additional ranked retailer, netting out to a total of 200.

Initial signups using an OTA email address were completed the week of April 4, 2016 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, using both an OTA email address and a Gmail address (in case the otalliance.org domain was being processed differently). 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 the recent OTA Native Advertising transparency research and interviews with regulators and stakeholders, scoring criteria were refined this year, generally resulting in more rigorous scoring. The weighting of the criteria was not changed – as in 2015, 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 as in the previous two years, violation of CAN-SPAM / CASL caused automatic disqualification from Best of Class consideration.

Testing was completed using Microsoft Windows PCs running Windows 10, Microsoft Outlook 2013 via Office 365, and Gmail. Web pages were examined using Google Chrome, Microsoft Edge and Internet Explorer. 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.

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.

As a cautionary note, in general, regulations apply to where the consumer resides and not where a company may have a physical nexus. Therefore, it is in the marketer's best interest to collect at signup the State/Province and Country where a user resides and to re-validate this data at least annually. While not part of this research, consumers have significant concern about list sharing. OTA did not evaluate the possibility of any list sharing during the analysis. Pending funding this may be incorporated into future years' research, including use and tracking of individual email addresses created for each of the 200 retailers.

SUMMARY

Email marketing continues to grow, engaging users globally. At the same time the levels of abuse and risks of fraud are undermining the vitality of this marketing channel. Many users are becoming overwhelmed with marketing messages flooding their inboxes across multiple devices. In fact, they are increasingly self-imposing an email detox by abstaining from their inbox. This sensory overload or "email fatigue" can disenfranchise potential customers.

As online publishers are observing a rise in ad blocking and faced with concerns regarding the transparency of native advertising and issues of privacy. Email marketers need to heed these trends as they relate to the trust of the email channel. While ad blockers were first dismissed by many, today they are having a material impact to online ad revenues. This underscores the importance that industry needs to put the consumer experience first, before trust in the inbox hits an inflection point.

This analysis confirms that the vast majority of top online retailers follow best practices beyond mere compliance. The number and type of companies receiving perfect scores shows that OTA's recommendations are within reach of all companies.

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. To maximize consumer trust, organizations must continually monitor marketing and subscription practices. As noted in the report, organizations should regularly test both their subscription processes and their unsubscribe processes to ensure ongoing conformity.

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. Companies found to be in violation could be fined up to 4% of global revenues.

Many third-party programs and services are available to assist organizations with compliance and honoring of opt-out requests, including areas such as email list suppression, list seeding, affiliate monitoring, list acquisition strategies and recipient feedback loops. Organizations may also consider services in areas such as user engagement surveys and preference center design, employee training and testing to help optimize marketing impact.

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

Guidance on Implied Consent http://www.crtc.gc.ca/eng/com500/faq500.htm

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

Yes Lifecycle Marketing - http://yeslifecyclemarketing.com/

Yes Lifecycle Marketing, Registration Best Practices - http://www.yesmail.com/resources/webinar/next-generation-registration-pages-emerging-trends-and-best-practices

Yes Lifecycle Marketing, Trigger Report - http://www.yesmail.com/resources/whitepaper/ultimate-email-trigger-report-12-triggers-boost-revenue

ACKNOWLEDGEMENTS

The research paper is a collaborative work product reflecting input from industry leaders and government agencies in Australia, U.S., Canada, England, Germany, Netherlands, New Zealand, Singapore and Switzerland Industry input has been provided by Act-On Software, Agari, American Greetings, Basegrow, Epsilon, Constant Contact, Harland Clarke Digital, Dmarcian, LashBack, Iconix, Marketo, Microsoft, OPTIZMO, Publishers Clearing House, Relevancy Group, Symantec, ThreatWave, UnsubCentral, ValiMail and Yes Lifecycle Marketing.

Funded In part from a grant from Yes Lifecycle Marketing

ABOUT THE ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a 501c3 charitable non-profit with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its sponsors and supporters include leaders spanning public policy, consumer protection, technology, e-commerce, social networking, mobile, email and interactive marketing, financial services, government, NGOs and industry organizations. To learn more visit https://otalliance.org

ABOUT YES LIFECYCLE MARKETING

Yes Lifecycle Marketing provides solutions that orchestrate cross-channel marketing communications to drive results and revenue. This is accomplished by leveraging technology, data, analytics, creative, and strategy to activate and optimize insights-driven, real-time, relevant communications. This holistic approach gives marketers the ability to source a full-service offering of best-of-breed technology and solutions from a single vendor in order to achieve their desired outcomes across all on and offline channels. To learn more visit www.yeslifecyclemarketing.com.

APPENDIX – 2016 BEST OF CLASS

- 3 1800Flowers.com
- 2 1800PetMeds.com
- 3 1Sale.com
- adidas.com
- AdvanceAutoParts.com
- 3 AE.com
- Aeropostale.com
- 3 AmericanGirl.com
- 3 Art.com
- ASOS.com
- AutoZone.com
- 3 Avon.com
- 3 Barneys.com
- 3 BassPro.com
- 3 Beachbody.com
- 2 BedBathandBeyond.com
- 3 Belk.com
- 3 BestBuy.com
- BeyondTheRack.com
- 3 **BlueNile.com**
- BN.com
- 3 BonTon.com
- 2 BrooksBrothers.com
- Build.com
- 2 BuildDirect.com
- 3 **Carters.com**
- 3 **CDW.com**
- 3 ChildrensPlace.com
- Columbia.com
- 3 Costco.com
- 3 CrateandBarrel.com
- Crutchfield.com
- CVS.com
- Cymax.com
- DeepDiscount.com
- 3 DisneyStore.com
- DuluthTrading.com
- 2 eBags.com
- 3 EddieBauer.com
- 2 EdibleArrangements.com
- 3 Etsy.com
- 2 **Evine.com**
- 3 Fanatics.com
- FocusCamera.com
- 3 FootLocker.com
- Fossil.com
- FragranceNet.com
- 3 Gap.com
- 3 Gilt.com
- 2 Groupon.com/Goods
- 2 Honest.com
- 3 **HSN.com**
- 3 JCP.com
- 3 JCrew.com
- 2 **Jomashop.com**
- 3 JPCycles.com
- JustFab.com
- 3 Karmaloop.com
- 3 KateSpade.com
- 3 Kay.com
- 2 Keurig.com
- Kroger.com
- Lakeside.com
- 3 LampsPlus.com
- 2 **LandsEnd.com**
- 2 Lenovo.com
- Levi.com
- 2 Lowes.com
- 3 LuluLemon.com
- 3 Macys.com
- MensWearhouse.com
- MidwayUSA.com
- 3 MilesKimball.com
- 2 ModCloth.com
- 3 Monoprice.com
- MusiciansFriend.com
- 2 NeimanMarcus.com
- 2 Newegg.com
- 3 NFLShop.com
- 3 Nike.com
- 3 Nordstrom.com
- 3 NorthernTool.com
- 2 Nutrisystem.com
- 3 OfficeDepot.com
- 3 OmahaSteaks.com
- 2 OneKingsLane.com
- 3 OpticsPlanet.com
- 3 OReillyAuto.com
- 3 OrientalTrading.com
- 3 Orvis.com
- 3 Overstock.com
- PotpourriGift.com
- 2 Puritan.com
- QVC.com
- 3 REI.com
- 2 RevolveClothing.com
- 2 RueLaLa.com
- 2 Sears.com
- 2 SearsOutlet.com
- ShoeMall.com
- Shoes.com
- Shop.MLB.com
- 2 Shop.Safeway.com
- 2 ShopJustice.com
- 3 Shopping.HP.com
- 3 **SierraTradingPost.com**
- 3 **Sweetwater.com**
- 3 Talbots.com
- 2 Target.com
- 3 TheBay.com
- 3 TheNorthFace.com
- 3 TheShoppingChannel.com
- 3 Tiffany.com
- 3 TireRack.com
- 3 ToryBurch.com
- ToysRUs.com
- 2 **ULTA.com**
- 3 UnderArmour.com
- UrbanOutfitters.com
- 3 VictoriasSecret.com
- 2 Vistaprint.com
- 3 **Walgreens.com**
- 3 Walmart.com
- WarbyParker.com
- 3 **Wayfair.com**
- 2 WBMason.com
- 2 WeightWatchers.com
- 2 Zazzle.com

2 3 – Number of consecutive years as Best of Class

Bold = Perfect Score