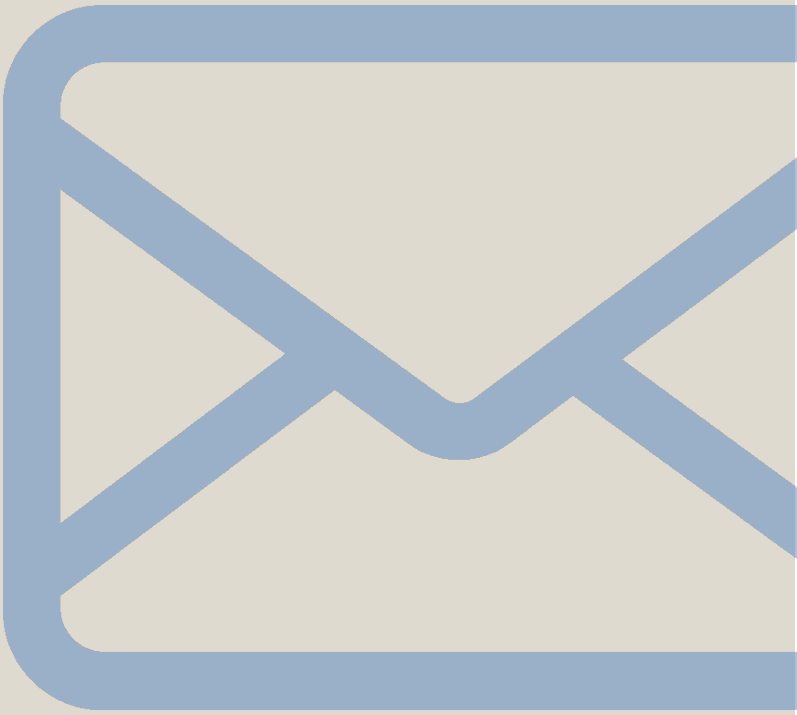


2018 Email Marketing & Unsubscribe Audit

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

OTA
Online Trust Alliance
an **Internet Society** initiative

Released November 28, 2018

Table of Contents

Background

Since its founding in 2005, the Internet Society's Online Trust Alliance (OTA) has regularly published benchmark reports promoting best practices to increase trust in various aspects of online interaction, while simultaneously recognizing organizations that have demonstrated excellence in their commitment to online trust and user empowerment. OTA became part of the Internet Society in 2017 and this best practice advocacy and reporting tightly aligns with the Internet Society's mission to ensure an open, globally-connected, secure, and trustworthy Internet for everyone.

Developing and accelerating the adoption of best practices to help bolster the integrity of interactive marketing is one of OTA's areas of focus. Email continues to be the preferred channel for consumers to interact with companies, and is deeply integrated into our daily lives. However, there are several factors that frustrate them, including issues with the frequency and relevance of email, leading them to consider other ways to interact with brands.[1]

In a continuing series of benchmark reports, OTA has initiated the 5th annual Email Marketing & Unsubscribe Audit, assessing the end-to-end user experience from signup through the mailing, unsubscribe process and results. 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.

Starting in 2014, working with multiple stakeholders, including the Federal Trade Commission, leading marketers, service providers and trade organizations, OTA developed and continues to update a list of best practices and associated scoring criteria for email marketing. 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. Leveraging learnings from the annual Online Trust Audit[2] and other OTA activity, the criteria and scoring are re-evaluated annually 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 one of stewardship, putting users first. OTA recommends the adoption of the outlined practices to respect consumers' preferences. Failure to do so risks organizations' brand reputation, deliverability and the possibility of regulatory scrutiny. Conversely, putting consumers first is the foundation for growth and long-term vitality.

[1] We Still Love Email, But We're Spreading the Love with Other Channels, https://theblog.adobe.com/love-email-but-spreading-the-love-other-channels/

[2] OTA Online Trust Audit, https://otalliance.org/TrustAudit

Executive Summary

The 2018 Audit found that the vast majority of audited online retailers have embraced unsubscribe best practices, going beyond mere compliance, and have shown continued improvement since 2014 despite expanded and more stringent criteria. This year's Audit examines the entire email engagement process, from signup to receiving email to the unsubscribe user experience and results.

Consistent with the four previous reports, the Audit focused on the top 200 North American online retailers.[3] For each site, analysts measured and tracked the signup process and user experience, and after observing emails received for as much as six months (and no less than one 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 insight into how to enhance the integrity of email marketing. Retailers achieving scores of 80% or higher received designation as "Best of Class."

For 2018, 74% of the top retailers qualified, a strong improvement from 67% in 2017 and nearly reaching the 75% achievement level of 2015. Primary drivers for the improvement were better discoverability of the unsubscribe link and increased use of encryption for the unsubscribe web pages. Ten of the audited retailers realized perfect scores – Dick's Sporting Goods, Home Depot, Lands' End, Musician's Friend, Office Depot, Optics Planet, Sierra Trading Post, Staples, Talbots and Walgreens.

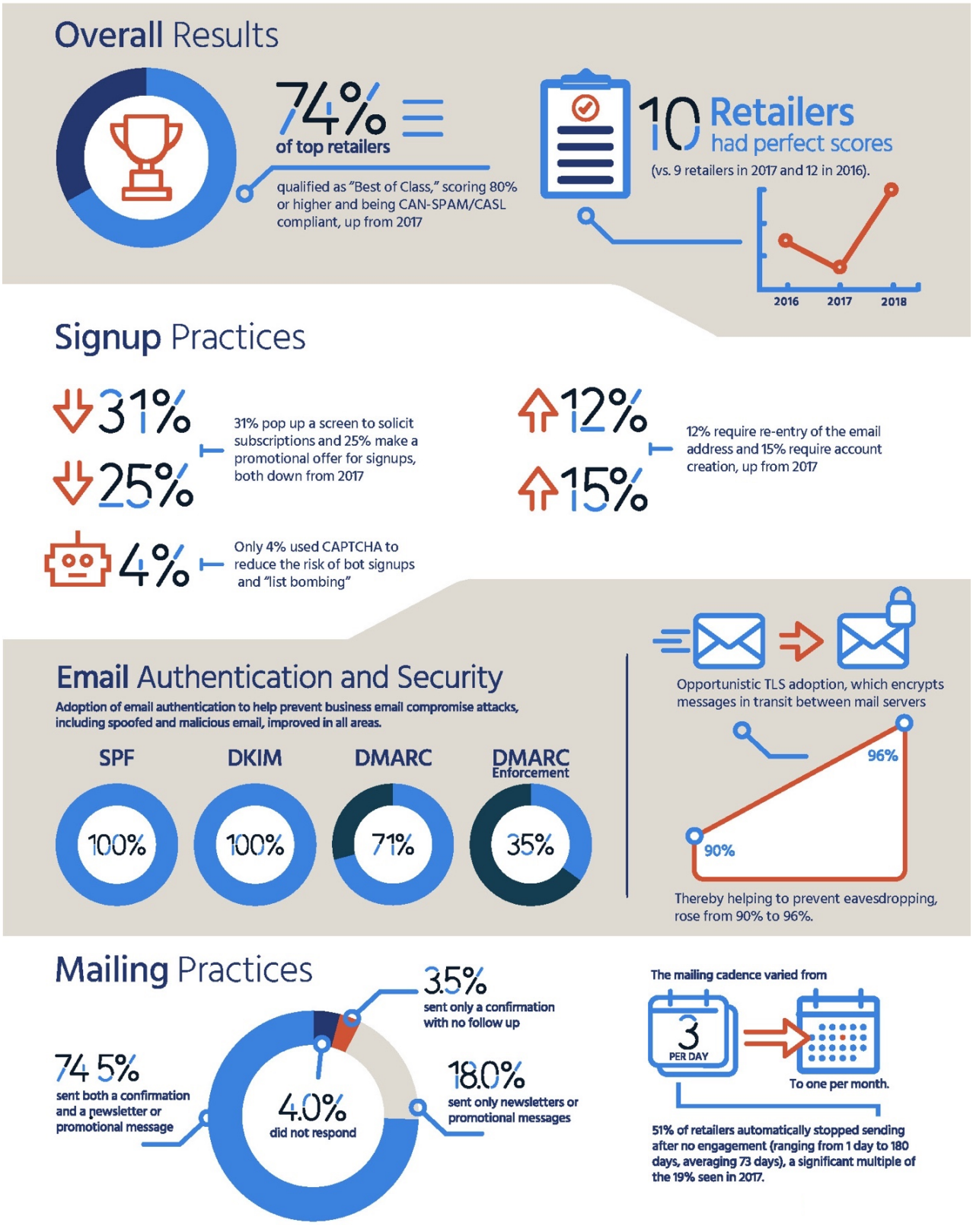
Email security was another highlight area in 2018. Adoption of email authentication technologies SPF and DKIM reached 100%, and adoption of DMARC (another email authentication technology to prevent spoofing) and opportunistic TLS (encrypting messages between mail servers) improved significantly.

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.[4]

[3] Source: Internet Retailer®, https://www.digitalcommerce360.com/product/top-500-database/

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

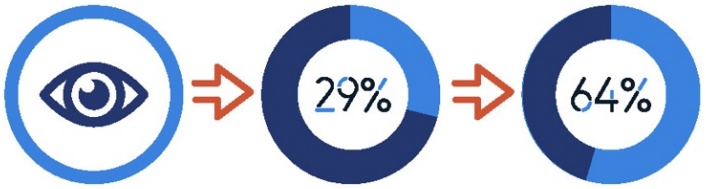
Key Findings



Unsubscribe Practices

Clear and conspicuous unsubscribe links were observed in 84% of retailer emails, a significant improvement after a steady decline to 76% in 2017.

Small text sizes for the unsubscribe link were used by one-third of retailers, but 10% increased text size to exceed minimum guidelines.



Readability of unsubscribe links improved slightly,

Though 29% still had unsubscribe text with contrast ratios below minimum W3C guidelines

And 64% were below W3C enhanced guidelines

For **77%** of Retailers the word UNSUBSCRIBE itself was the link to click

used an encrypted session for the unsubscribe page, an increase from 52% in 2017. Encryption prevents the email address and other information from being sent "in the clear."

29% set an expectation for the unsubscribe timeframe, ranging from "next few minutes" to 10 days, averaging 5.8 days, all improvements over 2017.

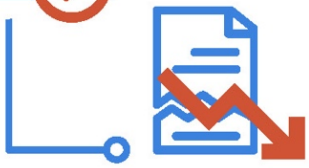
53% of retailers presented the unsubscribe link in a standalone single-word footer

24% presented it as part of a standalone sentence

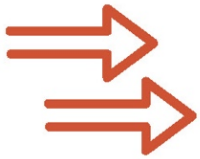
23% presented it within a paragraph of text, making it harder to find.

Unsubscribe Results

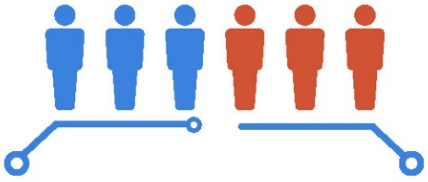
stopped sending messages immediately after the unsubscribe request was submitted (versus waiting the permitted 10 days), an improvement from 88% in 2017 and 86% in 2016.



Total violations of CAN-SPAM / CASL were 3.2% (6 retailers), a reduction by nearly half compared to 5.7% (11 retailers) last year.



Three mailed more than 10 days past the unsubscribe request, a drop from 8 in 2017 and 11 in 2016.



Three did not list a physical address in their email as required by CAN-SPAM and laws in other countries (consistent with 2017).

Signup Practices

The testing process entailed visiting each retailer's website intending to subscribe to newsletters or promotional email, and observing the entire process and user experience. This year's Audit continues the tracking of additional signup practices started in 2017. These 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. In the course of conducting the 2018 Audit, several new trends were noted this year that may be added to future reports. The results are shown in Figure 1 below.

SIGNUP PRACTICES			
	2016	2017	2018
Invitation			
Signup on Home Page	-	97%	100%
Signup at Top of Home Page	-	8%	6%
Easy to Find	-	85%	94%
Pop-Up Invitation to Subscribe to Email	34%	31%	31%
Promo Offer on Screen for Signing Up	31%	28%	25%
Signup Confirmation on Screen	89%	97%	98%
Data Entry			
Required Email Address to be Re-entered	16%	11%	12%
Requested Additional Information	41%	36%	40%
Required	-	28%	29%
Optional	-	19%	21%
Required Location	-	17%	14%
Required Account Creation	20%	11%	15%

Figure 1 - Signup Practices, 2016-2018

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 (explained on page 14). This year saw a sharp increase in signups that were "easy to find," growing to 94% from 85% last year. While not measured, it was noted that several sites included multiple subscription links – on the page header, within menu navigation and in the footer of the page.

As shown in the example on Figure 2, 31% of retailers encourage signup through homepage overlays or pop-over windows, flat to last year. Most have a signup box or link on the home page, typically either in the upper (header) area (6%, down from 8% in 2017) or the lower (footer) area of the page.

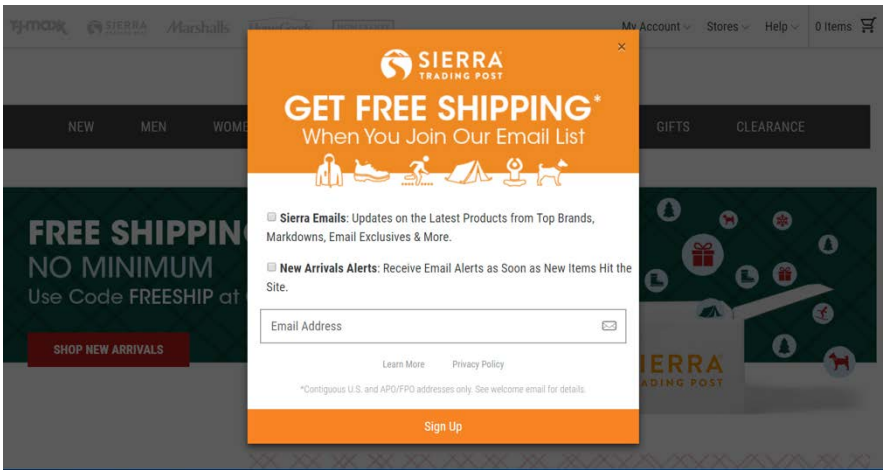


Figure 2 – Example of Pop-Up Window Inviting Subscription

Subscriptions were also solicited by offering a promotion or signup incentive (e.g., free shipping, discount on first order). Such incentives were offered by 25% of the sites (down from 28% in 2017 and 31% in 2016) – 64% of these sites also made an offer via a welcome email, down from 71% last year. Reiterating an offer or promo code both on screen and in an email is an opportunity to engage and drive purchases, though many retailers applied the coupon to the subscriber's cart upon signup, encouraging immediate purchases. 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 98% of retailers. Though only 2% did not confirm the subscription, it leaves the subscriber hanging, wondering if their action took effect.

Data Entry

Entering an email address is all that is necessary to initiate a subscription, but 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 modest increase in the amount and depth of interaction required for signups this year (except for location information, which decreased). This increase somewhat offsets the sharp decline seen in most categories from 2016 to 2017. Twelve percent of retailers required the email address to be entered twice (up from 11%). The purpose of this practice is to minimize entry errors, but today's real-time verification or real-time hygiene solutions can also address this issue.

Forty percent requested additional information about the subscriber (up from 36%), and 15% required account setup (up from 11%, though this requirement clearly varies by business model). Of the 36% that requested information beyond the email address, 29% required additional information to complete the subscription and 21% asked for optional information (some requested both required and optional information, which explains why the total exceeds 40%).

Of increasing concern is the low percentage of retailers requiring geographic information (only 14%, down from 17%), especially given that the EU's General Data Protection Regulation (GDPR) went into effect earlier this year 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 subscriber'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 to customize mailings, OTA advocates the prompting over time, with a clear emphasis that it is voluntary, not required. Conversely, requiring extensive information at initial sign up may cause the subscriber to abandon the process. Creating the ability to "tune" emails provides users more relevant email communications, and it was noted that several retailers offered these choices via icons this year (vs. the traditional text-based approach).

Subscriber Validation

The industry has not seen a recent repeat of 2016's "list or subscription bombing" attacks, in which consumers received hundreds of unsolicited emails within minutes, effectively incapacitating users' email accounts.[5] Still, OTA recommends that sites consider two simple practices to reduce the impact of such attacks.

CAPTCHA. The use of CAPTCHA (as shown in Figure 3) can help verify that the subscriber is a real person and not a bot.[6] While this does not 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 themselves requested the subscription.

While COI can significantly reduce signup abuse, it can also reduce legitimate registrations since such the confirmation email may be ignored, junked or discarded. Marketers have been reluctant to embrace this practice, keeping COI adoption very low.

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

[6] A challenge-response test to prevent bot signups, https://en.wikipedia.org/wiki/CAPTCHA

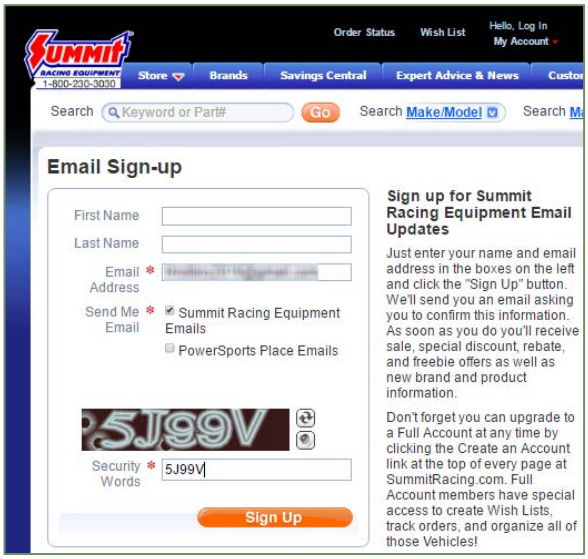


Figure 3 – Example of CAPTCHA

Results from this year's subscriptions are shown in Figure 4 below. Use of CAPTCHA grew slightly to 4%, while use of COI during the subscription process jumped significantly to 7%. Analysts noted that much of this increase was tied to new retailers on the list who are primarily based in the EU, and it is likely that their practice of employing COI in their home region has carried over to their U.S. activity. 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				
	2015	2016	2017	2018
Confirmed Opt-In (COI)	13.1%	6.0%	2.5%	7.0%
CAPTCHA	-	3.0%	3.0%	4.0%

Figure 4 - Subscription Validation Practices, 2015-2018

Mailing Practices

Similar to 2017, a complete range of data attributes were captured and analyzed this year to better understand retailers' email practices. Areas of analysis included: subscription results, promotions within confirmation messages, the mailing "cadence" (frequency of mailing), use of email authentication and server-to-server encryption for newsletters/ promotional messages.

Subscription Results

As shown in Figure 5, nearly 75% of marketers demonstrated the best practice of sending a signup confirmation and subsequent newsletter, a drop from the 2017 results. Eighteen percent skipped the welcome message and moved directly to newsletters/promotions. Nearly 4% sent a confirmation with no follow up, indicating a disconnect in the system. This is flat to 2017, and reflects a lost opportunity. Finally, 4% did not respond at all (up from none in 2017), indicating a complete breakdown in the system.[7] This is also lost opportunity.

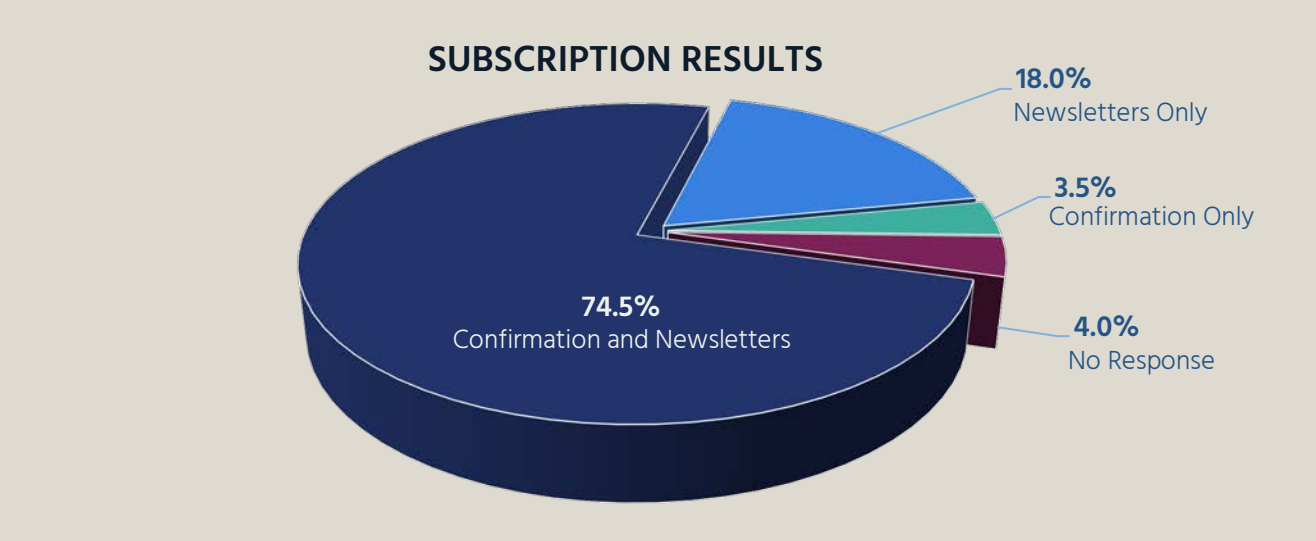


Figure 5 - Subscription Results, 2018

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 more than $12.5 billion between October 2013 and May 2018.[8]

[7] In instances where no confirmations or newsletters/promotions were received or only a confirmation was received, a second or even third 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.

[8] Business Email Compromise, the $12B Scam, https://www.ic3.gov/media/2018/180712.aspx

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.

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 major 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	2018
SPF	94.1%	95.3%	100.0%
DKIM	97.9%	99.0%	100.0%
DMARC Record	50.5%	59.6%	71.4%
Quarantine Policy	3.2%	4.7%	3.8%
Reject Policy	21.8%	28.0%	31.4%
Use of Opportunistic TLS	31.9%	89.6%	95.7%

Figure 6 - Email Authentication & Security, 2016-2018

This year we observed a key benchmark, with 100% of retailers using both SPF and DKIM. Looking more deeply at the DKIM support, 79% use the SHA-256 hashing algorithm, while 21% still use SHA-1, which is weaker. This will be explored further in future OTA email authentication reports. Adoption of DMARC also continued to grow significantly, topping 71%. Nearly half of the retailers using DMARC have an enforcement (quarantine or reject) policy.

Use of opportunistic TLS increased another 6% and is approaching the 100% level. A total of 92.4% of retailers use TLS 1.2, while 3.3% use TLS 1.0. This will also be explored further in future OTA reports. 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.

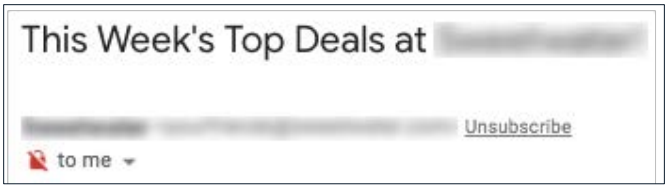


Figure 7 – Example of Gmail TLS Indicator

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 three messages per day to once a month, averaging a message every 2.5 days. Approximately 20% of retailers varied their cadence as time went on, often starting with messages every few days, then backing off to every several days or even weekly. This was often combined with several "pauses" over time, which varied in length from a week to a month.

In addition, 51% of retailers who sent email starting in April actually stopped sending entirely (without an unsubscribe) after a period of time, which varied from 1 day to 180 days, averaging 73 days. These are all increases from 2017, when only 19% of retailers stopped automatically in an average of 53 days.

This high degree of variance in cadence and duration of mailing highlights the difficulty marketers face when dealing with seemingly disengaged subscribers – do I keep sending unabated and risk spam complaints or do I modify the cadence in an effort to stay in front of the subscriber? Ultimately over half of the retailers chose to stop sending after some period of time, taking the subscriber's silence as an implied unsubscribe.

Unsubscribe Practices

The unsubscribe process and associated user experience have represented the primary analysis and reporting focus since the inception of this report in 2014. 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 resulting findings and analysis 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.** The unsubscribe 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 element 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 unsubscribe 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, 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.

   Though historically most email messages and websites had white backgrounds with dark text, many have recently switched to light grey backgrounds with grey or blue fonts. 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.[9] 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.[10] Including the header allows ISPs and automated unsubscribe services to easily identify the sender's opt-out mechanism. Gmail, Microsoft Outlook, Yahoo! Mail and other leading ISPs and mailbox providers display an unsubscribe button (or link) 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. 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.** Present the customer with 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 option 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 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.** 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.

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

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

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

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). 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 take effect 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 to 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. The Internet Society strongly advocates use of encryption to improve trust in the Internet.[11]

[11] The Internet Community Stands up for Encryption, https://www.internetsociety.org/encryption/internet-community-stands-up-for-encryption/

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). Because consumers may move outside of the U.S., marketers should adhere to the longest appropriate standard.

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. **Mailing lists 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 involving 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 improving 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.[12]

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. This is especially important given the General Data Protection Regulation (GDPR) that went into effect in the EU earlier this year.

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.[13]

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 jurisdictions apply to their subscriber base. This too is especially important in light of GDPR.

[12] Cyber Incident & Breach Readiness Guide – https://otalliance.org/Incident

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

Results: Disclosure, Discoverability & Delineation

The major finding in this area was a significant increase in "clear and conspicuous" links, which reverses a downward trend of several years. The "clear and conspicuous" criterion incorporates a combination of factors related to the discoverability of the unsubscribe link. The ease with which users can find the link is impacted by placement, surrounding text and graphics, color/contrast/size and use of terms. In fact, all criteria in this area improved except use of the unsubscribe header.

AUDITED & SCORED BEST PRACTICES - IN THE MESSAGE				
	2015	2016	2017	2018
Easily Read / Size	98.4%	92.6%	93.8%	95.1%
Commonly Understood Terms	94.0%	88.8%	91.7%	93.5%
Unsubscribe Header	85.2%	88.8%	92.2%	88.1%
Clear and Conspicuous	97.3%	81.4%	75.9%	83.8%

Figure 8 - Adoption of Scored Criteria in the Message, 2015-2018

Starting in 2017, additional data was collected to examine three additional aspects of discoverability – the placement of the link (standalone single-word footer menu vs. standalone sentence vs. part of a paragraph); the precise size and color contrast of the unsubscribe link text; and whether the link to click was actually the word "unsubscribe" (or equivalent) vs. other generic words elsewhere 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 placement seen this year. Compared to 2017, placement of the link in a sentence dropped by 4% with equal portions moving to the standalone footer and paragraph.

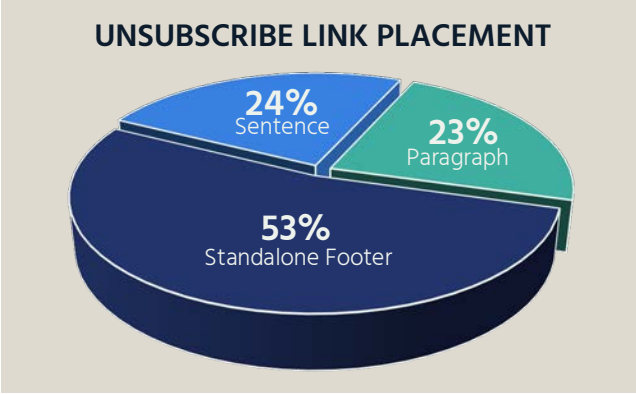


Figure 9 – Unsubscribe Link Placement, 2018

Privacy Policy | Unsubscribe | View Web Version

Example A – as part of a standalone footer

If you no longer wish to receive emails from us, you can unsubscribe at any time.

Example B – as a standalone sentence

You've received this message because you've registered or accepted our invitation to receive e-mail from [redacted]. If you'd like to update your preferences (contact frequency, product preference, etc.) or Unsubscribe from our [redacted] email list, you may click here.

Example C – in a paragraph

Figure 10 – Examples of Unsubscribe Link Placement

Unsubscribe Link Text Size. Precise text size for the unsubscribe link was tracked for the first time in 2017. It was tracked again this year and the breakdown is shown in Figure 11. From a scoring standpoint, sizes less than 10px do not receive credit, while text 10px or larger receives credit. For reference, 12-point type in print equates to 16px text on a website, and most experts recommend type sizes in the 12px-16px range for ideal readability of body text. Though the percentage of sites using text sizes of 10px or less stayed the same, use of 11px text dropped nearly 10%, mostly in favor of text sizes above 12px.

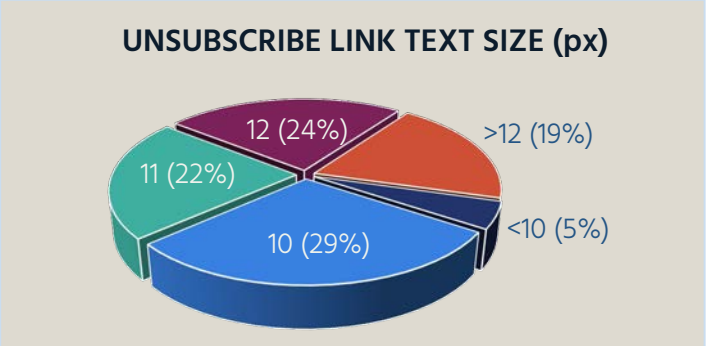


Figure 11 – Unsubscribe Link Text Size, 2018

Unsubscribe Link Contrast Ratio. The contrast ratio for unsubscribe link was also measured for the first time last 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, 29% of unsubscribe links observed were under the minimum guideline (a contrast ratio below 4.5:1 – 15% were below 3:1). Only 36% were above the enhanced guideline of 7:1.[14] This is a modest improvement over 2017 – 3% of sites moved above the minimum guideline and 5% moved above the enhanced guideline.

"Unsubscribe" as Link. Another factor impacting discoverability is the location of the link itself within the text. To assess this, analysts tracked the word used as the unsubscribe link. In total, 77% of messages used the word "unsubscribe" or "opt-out" as the link to click (vs. 76% in 2017, and only one retailer used "opt-out"). The remaining messages used "click here" or other words as the link. In general, this makes the link harder to find since the entire sentence must be read to understand what "click here" refers to, and the bottom of most marketing emails 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.

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

You may unsubscribe or update your email preferences at any time.

Example A – link not clear and conspicuous (this is a sentence, but the link has no distinction)

If you don't want to receive marketing messages from us, let us know.

Example B – poor terms

Figure 12 – Examples of Poor Disclosure, Discoverability and Delineation

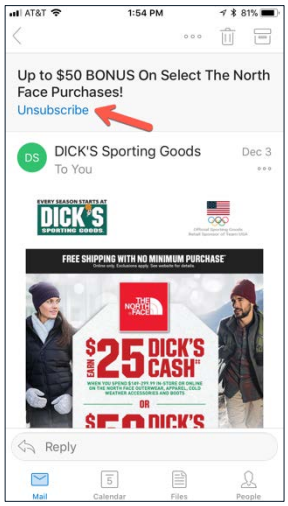


Figure 13 – Example of Unsubscribe Header Link in Mobile Client

Use of the unsubscribe header dipped this year, from 92% to 88%. This was primarily due to new retailers on the list, which only have 71% adoption of the unsubscribe header. 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

Results: Unsubscribe Process

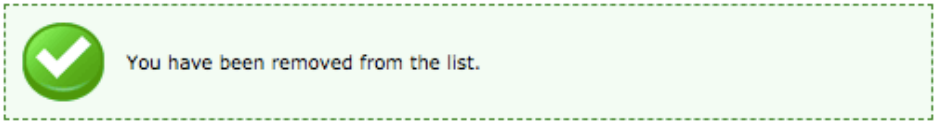
Figure 15 below lists best practices for the unsubscribe process. These include 1) the ability to opt out of all email, 2) landing on a branded page confirming the unsubscribe, 3) pre-population of the unsubscribe address, 4) presentation of a preference center / opt-down choice during the process and 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				
	2015	2016	2017	2018
Opt-Out All Email	97.3%	99.5%	99.5%	100.0%
Confirmation Web Page	94.5%	98.9%	100.0%	100.0%
Branded Page	90.2%	92.6%	93.3%	92.2%
Pre-Populated Unsubscribe Address	*90.7%*	*92.0%*	95.3%	89.7%
Preference Center and/or Opt-Down	61.7%	58.5%	58.5%	55.7%
Preference Center	55.7%	37.8%	37.8%	34.6%
Opt-Down	44.8%	33.0%	33.2%	34.6%
Optional Customer Feedback	24.0%	22.9%	20.2%	16.8%
Encrypted Unsubscribe Page	-	-	51.8%	68.6%

Figure 15 - Adoption of Scored Criteria in the Unsubscribe Process, 2015-2018 [15]

Overall Experience. As in previous years the unsubscribe experience ranged from abrupt, non-branded one-click interaction to elegant, branded experiences that presented various choices and solicitation of feedback. In general, retailers seem to be streamlining the unsubscribe process (seen in the drop in preference center/opt-down and customer feedback options), though the majority of retailers offer a link to change preferences as an alternative to presenting the consumer with a choice on the unsubscribe screen itself (this will likely be tracked in future Audits).

As in previous years, several retailers presented a "please subscribe" pop-up during the unsubscribe process, which is clearly a contradiction of purpose (though it may happen due to lack of cookies on the test computer, this should be suppressed so as not to annoy or confuse the user). Examples of extremes in experience are shown in Figure 16 below.



[15] Pre-populated unsubscribe address data from 2015 and 2016 is shown in italics since it was tracked but not a scored criterion.

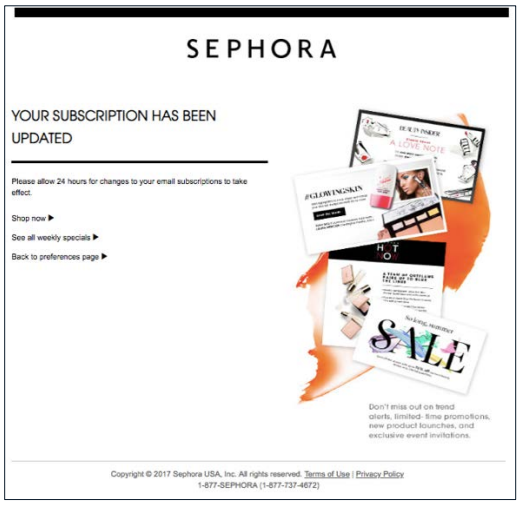


Figure 16 – Contrasting Examples of Branding in Unsubscribe Pages

Pre-Populated Unsubscribe Address. This was new to the scoring criteria in 2017, and its weight was increased this year. It is convenient for consumers and reduces errors, frustration and complaints since many consumers combine email in a common inbox and may not remember which email address they used to subscribe. Unfortunately there was a dip in adoption this year, even from retailers who were part of the Audit in 2017.

Encrypted Session to Unsubscribe Page. Also new in 2017 was tracking of encryption support on the unsubscribe web page. Adoption of this practice took a significant jump, from 52% to 69%, and corresponds with increased use of encryption on all web pages and opportunistic TLS between mail servers. Retailers should check whether their unsubscribe pages are encrypted, and if they are not, encourage their IT department or email service provider (ESP) to enable it.

Branded Unsubscribe Page. Ninety-two percent of retailers used a branded unsubscribe page this year, a slight drop from 2017. Some branding was very simple, while others were elaborate – marketers should ensure that the user's unsubscribe experience is in line with their overall branding goals. Since the unsubscribe experience is often managed by ESPs, full integration of the branding experience can be challenging, but there is usually a way to accommodate marketers' needs.

Preference Centers/Opt-Down. Overall use of preference center and opt-down options was down slightly this year, with a dip in use of preference centers partially offset by a slight increase in use of opt-down options. A new opt-down option observed this year was "snooze" – the choice to pause email for some period of time (usually 30, 60 or 90 days). There are several means to determine consumers' interests outside the use of a preference center, but OTA encourages marketers to gives consumers choice and control to minimize list abandonment. For instance, as part of this year's Audit, after a long period of user inactivity several retailers sent messages offering the subscriber to engage with the company via email, social media or texts.

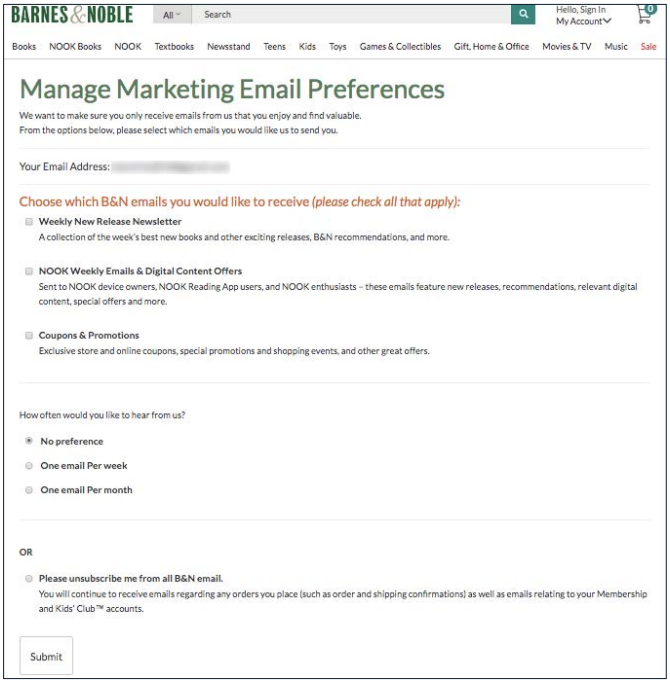


Figure 17 – Example of Preference Center / Opt-Down Choices

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 of this practice continued its steady decline, falling to 17%. Though this kind of feedback can be valuable to refine content and processes, it needs to be evaluated for actual user engagement and may be supplemented by social media and other forms of user interaction.

Setting Expectations for Unsubscribe Timing. As in 2017, analysts captured whether retailers offered an unsubscribe timing expectation (e.g., "You have been unsubscribed. Please give us 3 days to honor this request."). Use of this practice rose from 25% to 29%, with the average stated time rising from 5.6 to 5.8 days. Statements ranged from "next few minutes" (laudable, offered by Northern Tool) to the full 10 business days allowed by CAN-SPAM.

OTA encourages retailers to adopt this practice, especially when the expectation can be set much lower than the 10-day compliance standard. Given that 89% of retailers honor unsubscribe requests immediately, it seems that the vast majority could state a time much shorter than the 10 days allowed. Only two retailers sent messages beyond the number of days they stated – one stated one day but stopped after five business days while the other did not honor the unsubscribe request at all.

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 allowed 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 slightly to 89%. 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 the risk for 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 dropped to 1.1%. 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				
	2015	2016	2017	2018
Unsubscribe Confirmation Email	2.7%	2.7%	2.1%	1.1%
No Delay on Removal	83.1%	85.6%	88.1%	89.2%
Violate CAN-SPAM/CASL (total)	7.1%	5.9%	5.7%	3.2%
Failed to Honor Unsubscribe	1.6%	5.9%	4.1%	1.6%
Broken Unsubscribe Link	5.5%	0.0%	0.0%	0.0%
Physical Address not Listed in Email	-	-	1.6%	1.6%

Figure 18 - Unsubscribe Results, 2015-2018

Of the two companies who issued an unsubscribe confirmation email, both confirmed the unsubscribe request. One set an expectation for how long it would take to honor the request. Both offered a link to "change email preferences" if the recipient changed their mind or had unsubscribed in error. Neither included any promotional messaging.

The number of retailers that failed to honor the unsubscribe request dropped to 1.6% (3 retailers) from 4.1% (8 retailers) last year. Two were repeat offenders from 2017. The third immediately honored the unsubscribe request in 2017 and stopped promptly after the second unsubscribe request this year.

It is encouraging to see the improvement in honoring of unsubscribe requests, though any failures serve as a reminder that retailers should continually monitor unsubscribe processes to 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.

Starting in 2017, 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. One was a repeat offender, one did not have this issue in 2017 and one was new to the list this year. This is a basic requirement that can be easily corrected.

Email Industry Leaders

The 2018 Audit includes a "Best of Class" designation for retailers who scored 80% or better and were CAN-SPAM/CASL compliant. As shown in Figure 19, of retailers who sent newsletters / promotional messages, 74% achieved this distinction, a significant improvement from 67% in 2017.

The primary criteria feeding this improvement were increased discoverability ("clear and conspicuous" unsubscribe links) and increased use of encryption on the unsubscribe pages.

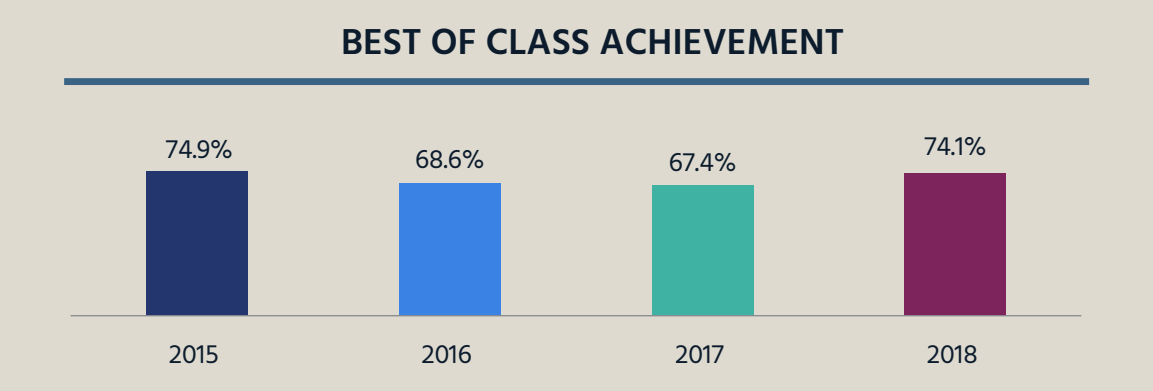


Figure 19 – Best of Class Achievement, 2015-2018

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 in 2017, but rose slightly to 10 this year. The retailers receiving perfect scores in 2018 were: DicksSportingGoods.com, HomeDepot.com, LandsEnd.com, MusiciansFriend.com, OfficeDepot.com, OpticsPlanet.com, SierraTradingPost.com, Staples.com, StitchFix.com, Talbots.com and Walgreens.com.

Five retailers repeated their perfect scores of 2017: LandsEnd.com, MusiciansFriend.com, SierraTradingPost.com, Talbots.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 Appendix C on page 30. Of those who did not repeat 2017's 100% attainment, two were not on the list this year and two no longer offered preference center/opt-down or customer feedback options.

As in 2017, analysts also looked at retailers who had full adoption of email authentication and security, as defined by supporting all of the following practices in their newsletter/promotional emails – SPF, DKIM, DMARC enforcement (a policy of reject or quarantine) and Opportunistic TLS. Overall, 34% had this full adoption (vs. 29% in 2017), and 43 (vs. 35 in 2017) of the "Best of Class" recipients were in this category. Appendix C on page 30 has a "^" next to each retailer who had full email authentication and security adoption. OTA recognizes that this does not necessarily imply that the same retailers have similar adoption on their corporate email or other email subdomains.

Summary

Email marketing is still a preferred channel for companies and consumers because it enables direct engagement with personalized, relevant content. Still, consumers complain about overloaded inboxes and are increasingly concerned about the validity of email they receive due to business email compromise and other phishing attacks. Given these consumer concerns and the regulatory shifts such as GDPR, email marketers need to focus on the consumer while providing them with expanded choice and control.

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 regarding use of data and consequences of choices via transparent disclosures; and
- protecting the integrity of email and websites through use of email authentication and encrypted email transfers and web sessions.

The 2018 results confirm that the vast majority of top retailers support these practices well beyond mere compliance levels. Significant improvements were seen in nearly every area – especially regarding discoverability of the unsubscribe link, honoring of unsubscribe requests and the securing of email messages and website interactions via email authentication and encryption. This resulted in a nearly record level of "Best of Class" achievement.

Still, there are still a few points of concern. Though the signup process continues to be streamlined to minimize friction, to support the new regulatory environment marketers need to strike the right balance and collect appropriate data (especially related to citizenship and residency) early in the process and set clear expectations about use of the data collected and consequences of consumers' choices. In addition, the decline in pre-population of the email address during the unsubscribe process increases consumer frustration, confusion and error rates, helping no one. Marketers should closely examine all recommended practices in light of the competitive environment established by their peers and make intentional decisions about whether and how to adopt these practices.

Overall, OTA commends marketers and email service providers (many of whom have contributed to the criteria and content of this Audit over the years) for their commitment to consumer empowerment and control of their inbox. 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.

Ultimately, marketers have a choice to make. Failure to keep up with best practices can lead to regulatory oversight, deliverability or placement problems and even lost business. Conversely, as marketers give consumers more choice, notice and control, trust will increase, enabling the email and marketing industry to continue to thrive. We all have a shared responsibility to continue to improve the integrity of the email channel, respecting input from all stakeholders.

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

Appendix A – Methodology & Limitations

OTA's Email Marketing & Unsubscribe Audit focused on the top 200 North American e-commerce sites based on revenue as of December 2017, as reported by Internet Retailer Magazine. In total, 27 sites on the list changed from 2017 to 2018, which is comparable to previous years. Most of the changes were due to shifts in ranking from year-to-year, consolidation and acquisitions. The remainder were tied to OTA analysts' qualifications to sign up on certain sites (e.g., many 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 217th ranked retailer) until a total of 200 subscriptions were made.

Initial signups utilized a Gmail address and were completed the week of April 2, 2018. Additional subscription requests were made in September and October for retailers who had not responded, had only sent a confirmation with no follow up, or who had stopped sending. Unsubscribe requests commenced in early October and were tracked through mid-November. If necessary, additional unsubscribe requests were issued during late October and early November.

Based on feedback from leading email service providers, regulators and stakeholders, scoring criteria were refined again this year, generally resulting in more rigorous scoring. The two new criteria added in 2017 – 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) – were given increased weight in 2018.

Criteria were weighted in three layers – the highest weight was given to "core" best practices, less weight was given to "advanced" best practices and the lowest tier included the new criteria from 2017. Weighting for "text size" and "terms used" was lowered from the top tier to the middle tier this year to allow increases in other areas and because their impact is also factored into the overall "clear and conspicuous" scoring. 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 primarily using MacBooks running macOS Sierra, Chrome and Gmail and was supplemented using Microsoft Windows PCs running Windows 10, Edge, Chrome and Gmail. Web pages were examined at a "Zoom" setting of 90%, 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 WCAG Contrast checker, both Chrome add-ins) were used to accurately measure 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.

Appendix B – 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)

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

Appendix C – 2018 Best of Class

- ❺ 1800Flowers.com
- ❹ 1800PetMeds.com
- ❸ Adidas.com ^
- Adorama.com
- ❸ AdvanceAutoParts.com
- ❺ AE.com
- ❸ Aeropostale.com
- AirCompressorsDirect.com ^
- ❷ AnnTaylor.com
- APMEX.com
- ❺ Art.com ^
- ❸ ASOS.com ^
- ❷ AutoPartsWarehouse.com ^
- ❸ AutoZone.com ^
- ❹ BedBathandBeyond.com ^
- ❺ Belk.com
- ❷ BlueApron.com
- ❺ BlueNile.com
- ❸ BN.com
- ❷ BodenUSA.com
- ❹ BrooksBrothers.com
- Brownells.com
- ❸ Build.com ^
- ❷ Cabelas.com
- ❷ CalvinKlein.com
- ❺ Carters.com
- Casper.com ^
- CDW.com
- Chicos.com
- ❺ ChildrensPlace.com ^
- ❸ Columbia.com
- ❺ CrateandBarrel.com
- Cricut.com
- ❸ Crutchfield.com
- ❸ CVS.com ^
- **DicksSportingGoods.com**
- Dillards.com
- DisneyStore.com
- DollarShaveClub.com
- ❸ DuluthTrading.com
- Dyson.com
- eBags.com ^
- ❺ EddieBauer.com
- ❹ EdibleArrangements.com ^
- ❷ EsteeLauder.com ^
- ❹ Evine.com
- ❺ Fanatics.com
- ❷ Fingerhut.com
- FinishLine.com
- ❺ FootLocker.com
- FragranceNet.com ^
- FreshDirect.com
- FTD.com
- ❷ GameStop.com ^
- ❺ Gap.com ^
- Glossier.com
- GNC.com
- ❹ Groupon.com ^
- ❷ **HomeDepot.com**
- ❹ Honest.com
- ❷ HP.com ^
- iHerb.com ^
- ❷ Ikea.com ^
- ❺ JCrew.com ^
- Jjill.com ^
- ❷ JMBullion.com
- ❹ Jomashop.com ^
- ❺ JPCycles.com
- ❸ JustFab.com
- ❺ Kay.com ^
- KEH.com
- ❹ Keurig.com ^
- KnifeCenter.com
- ❷ Kohls.com ^
- ❸ Kroger.com
- Lacoste.com
- ❸ Lakeside.com
- ❹ **LandsEnd.com**
- ❹ Lenovo.com ^
- LootCrate.com
- ❹ Lowes.com
- ❺ LuluLemon.com ^
- ❺ Macys.com ^
- ❸ MensWearhouse.com
- ❸ MLB.com
- Mouser.com
- ❸ **MusiciansFriend.com**
- Net-a-Porter.com ^
- ❹ Newegg.com ^
- ❺ NFLShop.com
- ❺ Nike.com
- ❺ Nordstrom.com ^
- ❺ NorthernTool.com
- ❹ Nutrisystem.com ^
- NYandCompany.com
- ❺ **OfficeDepot.com**
- OmahaSteaks.com
- ❺ **OpticsPlanet.com**
- ❺ OrientalTrading.com
- ❺ Overstock.com ^
- ❷ Patagonia.com
- ❷ Peapod.com
- ❹ Puritan.com
- ❺ REI.com ^
- ❷ RestorationHardware.com
- ❹ Revolve.com ^
- ❷ Rubbermaid.com
- RueLaLa.com
- ❹ Safeway.com
- ❹ Sears.com
- ❹ SearsOutlet.com
- ❷ Sephora.com
- ❸ ShoeMall.com
- Shoplet.com
- ❷ Shutterfly.com
- ❺ **SierraTradingPost.com**
- Sonos.com
- **Staples.com ^**
- SteelSeries.com
- ❷ StitchFix.com ^
- ❺ Sweetwater.com
- ❷ SwissColony.com
- ❺ **Talbots.com**
- Target.com
- ❷ TheRealReal.com ^
- ❺ TheShoppingChannel.com
- ThriveMarket.com
- Tiffany.com
- ❺ TireRack.com
- ❺ ToryBurch.com
- ❷ UGGAustralia.com ^
- ❺ UnderArmour.com
- ❹ Vistaprint.com
- ❺ **Walgreens.com**
- Walmart.com ^
- WarbyParker.com
- ❹ WeightWatchers.com

❷❸❹❺– 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

About the Online Trust Alliance (OTA)

The Internet Society's Online Trust Alliance (OTA) identifies and promotes security and privacy best practices that build consumer confidence in the Internet. Leading public and private organizations, vendors, researchers, and policymakers contribute to and follow OTA's guidance to help make online transactions safer and better protect users' data. The Internet Society is a global nonprofit dedicated to ensuring an open, globally connected, trustworthy, and secure Internet for everyone.

Rev1128