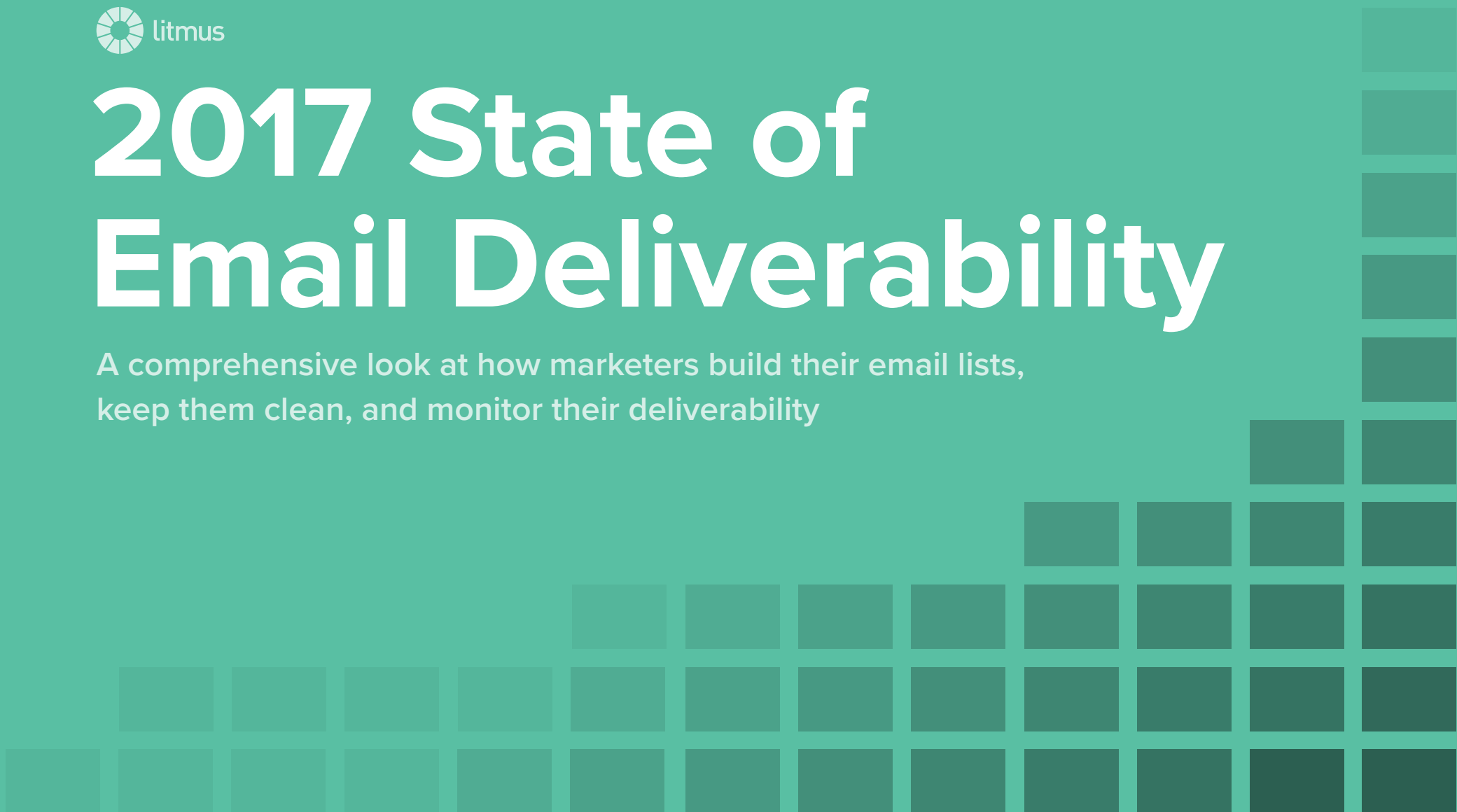




# 2017 State of Email Deliverability

A comprehensive look at how marketers build their email lists, keep them clean, and monitor their deliverability



Maintaining a strong sender reputation and high deliverability rates is critical to email marketing success. At least that is what we've been told. Our survey of thousands of marketers worldwide tells a slightly different story, one where blocks and blacklistings affect even successful companies.

For instance, marketers who describe their email programs as successful are only 19% less likely than those at less successful programs to have had their emails blocked in the past 12 months (31.6% vs. 38.8%). And successful programs are pretty much just as likely as other programs to be blacklisted.

When an inbox provider imposes a block on a sender, depending on the severity and breadth of the block, many of their emails will no longer be delivered to any of that provider's users. When a sender is blacklisted, generally their emails will be blocked by all of the inbox providers that subscribe to that blacklist and implemented in filtering decisions.

Even though deliverability problems don't stop email programs from being successful, that doesn't mean that marketers shouldn't do more to avoid blocks and blacklistings. These situations are avoidable, as certain practices clearly lower email marketers' risks, while others absolutely raise them—sometimes dramatically.

## In our first annual State of Email Deliverability report, we look at the deliverability ramifications of marketers':

Subscriber acquisition sources .....	<a href="#">5</a>
Permission practices .....	<a href="#">10</a>
Authentication .....	<a href="#">12</a>
List-unsubscribe and encryption usage .....	<a href="#">14</a>
List hygiene and spam filter tools .....	<a href="#">16</a>
Inactivity management.....	<a href="#">19</a>
Analytics and deliverability monitoring .....	<a href="#">24</a>

Use the results to benchmark your own acquisition, list hygiene, and deliverability practices, and to identify opportunities for improvement. Share the findings with your company's leadership to help advocate for more resources or changes in practices.

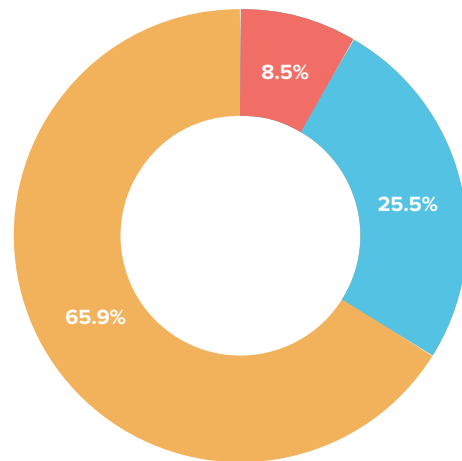
All of this is made possible by the more than 3,500 marketers who generously took the time to take our State of Email Survey and share their insights with the industry. For a breakdown of the demographics of our respondents, check out this [snapshot of the email professional](#).

Now, let's make our email deliverability better!

## Prevalence of Being Blocked

Have your company's marketing emails been blocked in the past 12 months or so?

1,643 respondents

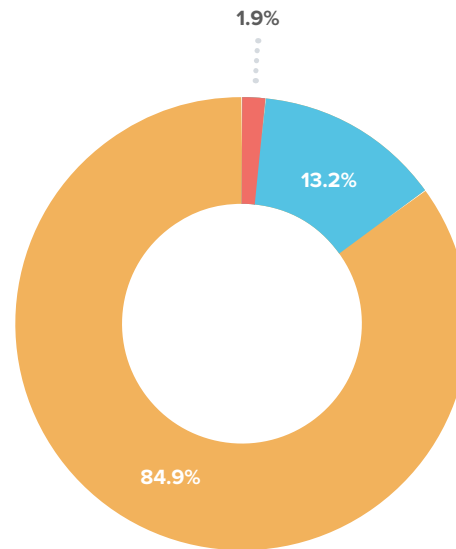


- Yes, we were blocked several times.
- Yes, we were blocked once or twice.
- No.

## Prevalence of Being Blacklisted

Has your company's marketing emails been blacklisted in the past 12 months or so?

1,683 respondents



- Yes, we were blacklisted several times.
- Yes, we were blacklisted once or twice.
- No.

## Key Takeaways & Action Items

A wide range of factors impact your email program's deliverability. Here are our top tips from the 2017 State of Email Deliverability report to help you get safely to the inbox:

### 1. Focus on optimizing 5-7 subscriber acquisition sources.

The best ones include signups on your homepage and social media pages; during checkout and account creation or registration; and at live and online events. Also, avoid using problematic sources such as list buying, list rental, and co-registration, which correlate to higher block and blacklisting rates.

**2. Fully authenticate your emails.** Use Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect your brand from spoofing and from having your subscribers receive security alerts about your emails. Less than 40% of brands use all three methods of authentication and all three should be used.

**3. Don't manually remove bounces.** Trust your email service provider to handle soft and hard bounces appropriately. If your ESP doesn't offer it, get a third-party provider bounce management solution. When brands handle it themselves, it's too tempting to find reasons to hold onto risky email addresses.

**4. Use spam filter and deliverability monitoring tools.** You can't fix deliverability problems if you're not aware of them. More than 42% of brands don't run spam filter tests before hitting send and 20.7% don't monitor their deliverability.

**5. Stop emailing chronically inactive subscribers.** Most inbox providers factor engagement into their filtering algorithms, so emailing subscribers who haven't opened or clicked in a long time will eventually impact your deliverability. More than 45% of brands never stop emailing inactives, a practice that progressively depresses your engagement.

### Improve Your Chances of Reaching the Inbox with Litmus

Litmus Spam Testing helps you identify and resolve potential deliverability issues before you press send. Explore Spam Testing and the entire Litmus platform so you can build, test, and analyze your email campaigns and take your email marketing program to the next level.

Activate your Litmus free trial coupon

Try Spam Testing through this special [free trial offer](#).



# Subscriber Acquisition Sources



The foundation of any list-building strategy is how and from where you attract your subscribers. Brands use 4.5 subscriber acquisition sources on average. However, marketers who describe their email programs as successful use closer to 5 subscriber acquisition sources (4.87), while less successful programs use closer to four (4.19). The exact sources used vary significantly by industry vertical.

The number of subscriber acquisition sources used correlates strongly with program success. Among brands using one to three sources, 36.9% said their programs are successful, compared to 43.2% using four or five sources and 50.2% using six or more sources.

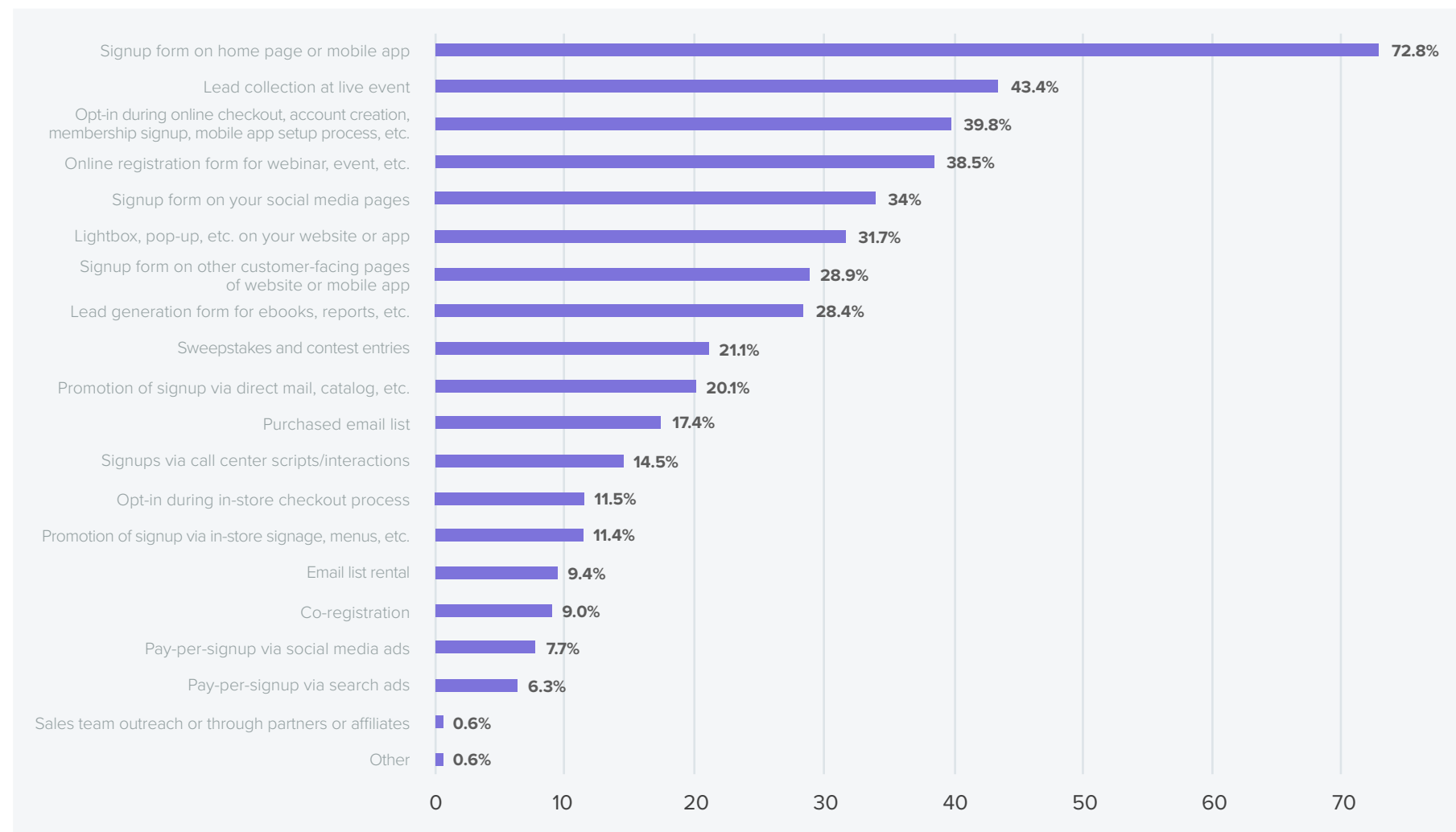
At the same time, brands that use more acquisition sources also experienced blocks and blacklistings at higher rates. Among brands using one to three sources, 30.7% said their emails had been blocked in the past 12 months and 12.0% said they'd been blacklisted. That compares to 36.2% and 16.8%, respectively, using four or five sources; and 38.1% and 19.3%, respectively, using six or more sources.

While using more subscriber acquisition sources offers more opportunity, it also presents more risk. Better email program funding partially offsets that risk, with 35.1% of programs using six or more sources saying they are well resourced versus less than a quarter of programs using five or fewer sources.

# Subscriber Acquisition Sources Used

Which of the following types of subscriber acquisition sources has your company used in the past 12 months or so? (Select all that apply.)

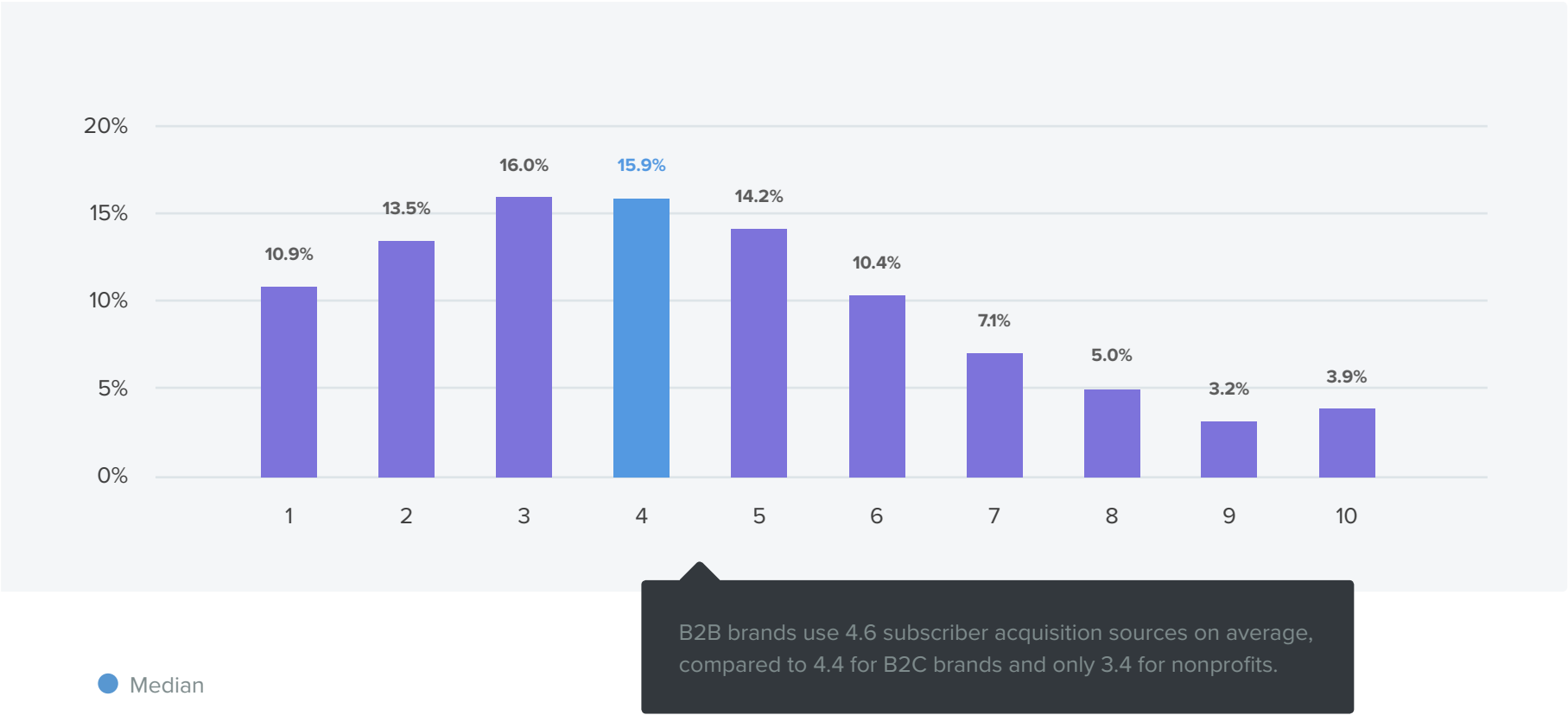
2,034 respondents



# Number of Subscriber Acquisition Sources Used

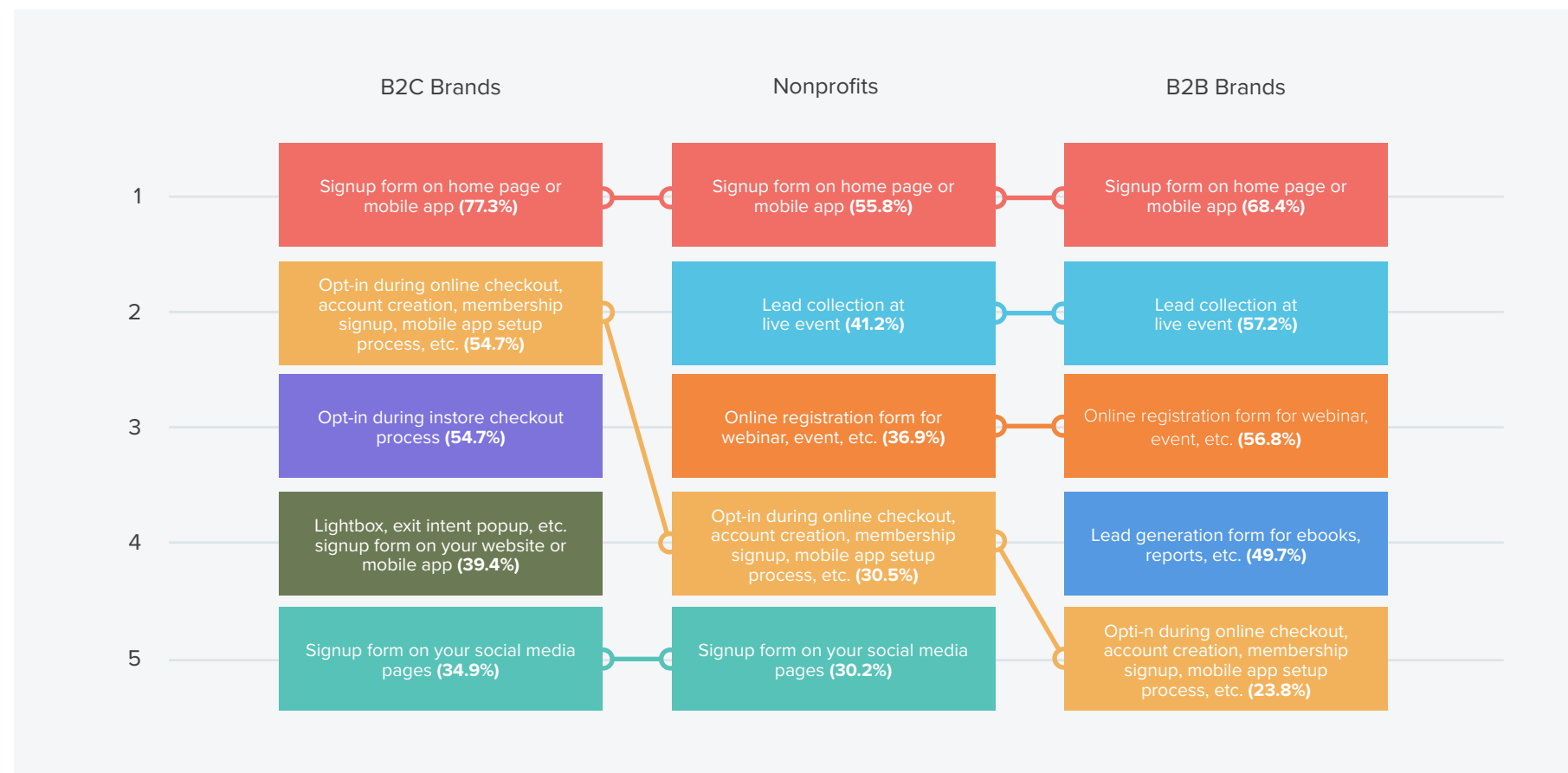
From among 20 subscriber acquisition sources provided

2,034 respondents



# Top 5 Subscriber Acquisition Sources

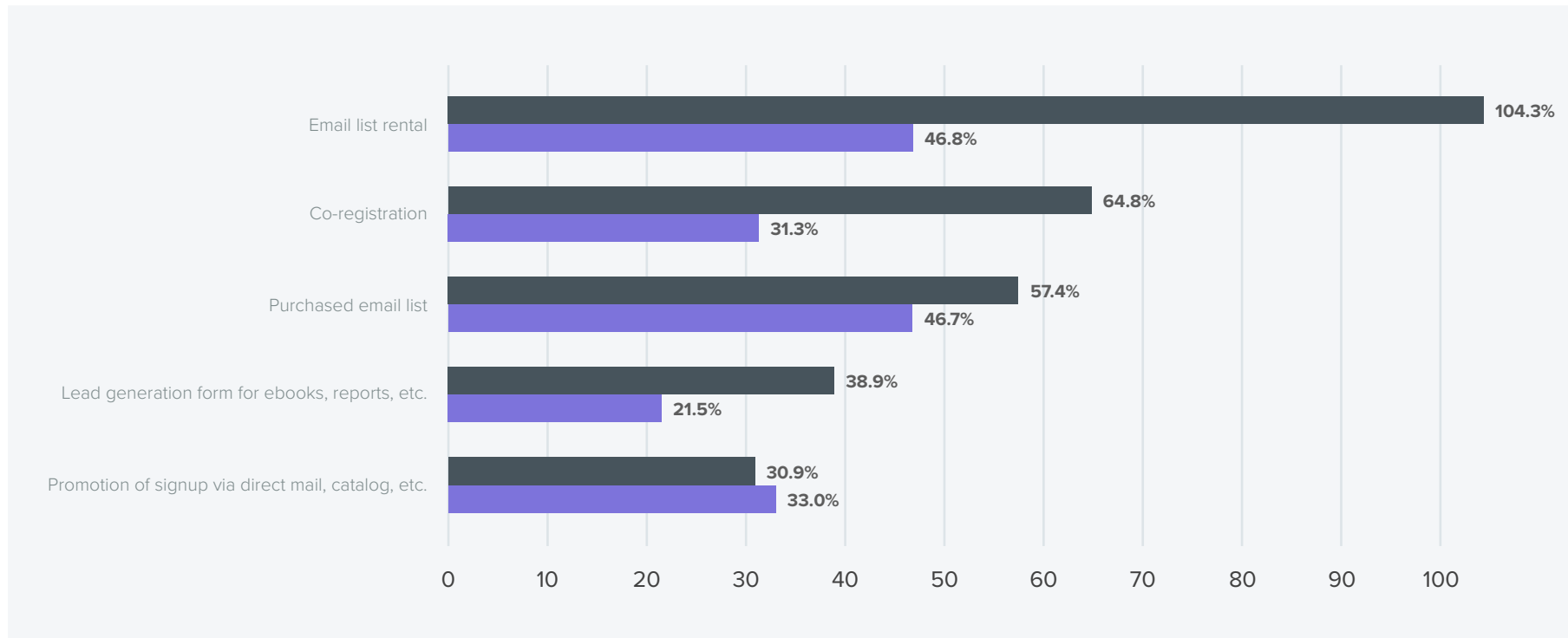
From among 20 subscriber acquisition sources provided





# Most Problematic Subscriber Acquisition Sources

For a closer look at these subscriber acquisition sources and whether any of them can be redeemed, check out [The 5 Most Problematic Subscriber Acquisition Sources: Are they redeemable?](#)



## ● More likely to be used by a blacklisted sender

How much more likely these sources are to be used by brands that have been blacklisted in the past 12 months compared to brands that haven't been blacklisted during that time

2,034 respondents

## ● More likely to be used by a blocked sender

How much more likely these sources are to be used by brands that have been blocked in the past 12 months compared to brands that haven't been blocked during that time

2,034 respondents



# Permission Practices

Double opt-in (DOI) has long been held up as creating much higher quality, lower risk email lists than single opt-in (SOI) because DOI includes a signup confirmation. Our research backs that up, but not nearly to the degree that we expected.

Brands that relied mostly on a double opt-in process were only 5.9% less likely than those relying mostly on single opt-in to report being blocked in the past 12 months. Plus, they weren't any less likely to report being blacklisted.

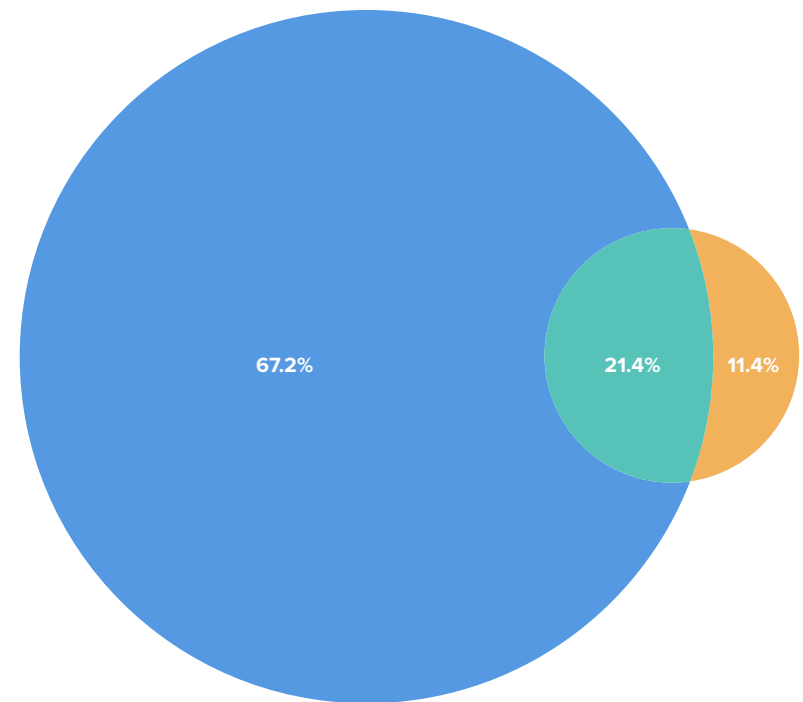
Inexplicably, brands that used a mix of SOI and DOI fared considerably worse in terms of deliverability than brands that mostly used SOI, with those brands being more likely to have been blocked (38.6% vs. 34.3%) and slightly more likely to have been blacklisted (17.5% vs. 15.4%) in the past 12 months.

# Signup Confirmation Practices

Does your company use mostly a single opt-in or double opt-in process?

1,899 respondents

For a deep dive into signup confirmation and permission practices, read our Single Opt-in Vs. Double Opt-in blog post series, which culminates with our [Verdict on Email Permission](#).



- All or mostly single opt-in
- A mix of single opt-in and double opt-in
- All or mostly double opt-in

# Authentication

Despite being created more than a decade ago to help senders detect spoofing, less than 70% of brands use Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

Domain-based Message Authentication, Reporting & Conformance (DMARC), which works with SPF and DKIM, is much newer, which partially explains why fewer than half of brands use it.

It's best practice to use all three. Successful and sophisticated email programs understand this.

Marketers who describe their programs as successful are more likely than those at less successful programs to use SPF (71.6% vs. 65.6%), DKIM (70.2% vs. 60.0%), and DMARC (54.5% vs. 36.3%). And marketers who describe their programs as sophisticated are even more likely to use SPF (77.4% vs. 62.9%), DKIM (76.2% vs. 58.6%), and DMARC (60.9% vs. 36.5%) when compared to marketers at less sophisticated programs.

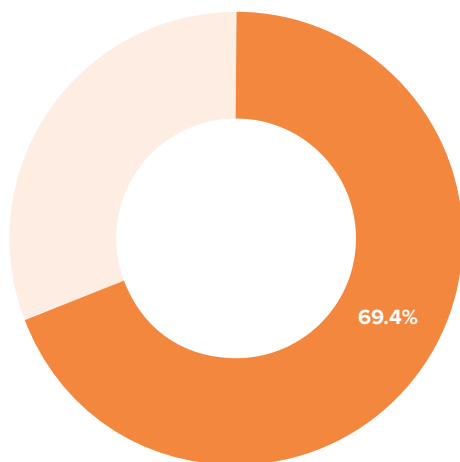
Surprisingly, smaller companies are using authentication at slightly higher rates than larger companies, which are more at risk of being spoofed. Companies with fewer than 500 employees were more likely than larger companies to use SPF (70.2% vs. 67.8%) and DKIM (67.5% vs. 64.6%), although larger companies were slightly more likely to use DMARC (48.7% vs. 45.3%).

DMARC is the newest authentication component. To better understand it, check out [DMARC: What It Is + How It Helps Protect Your Brand Against Email Fraud](#).

### SPF Usage

Does your company authenticate your marketing emails using Sender Policy Framework (SPF)?

1,217 respondents

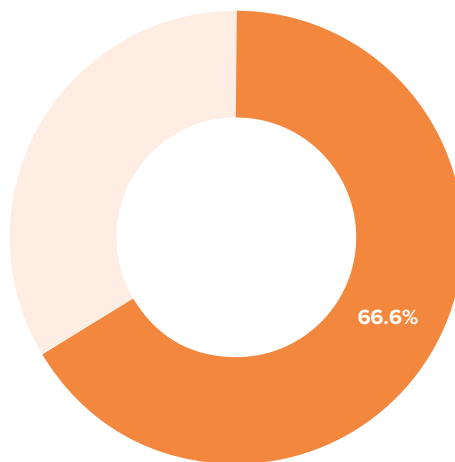


Yes.

### DKIM Usage

Does your company authenticate your marketing emails using DomainKeys Identified Mail (DKIM)?

1,223 respondents

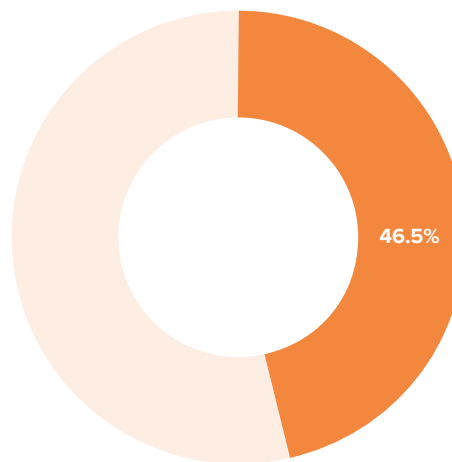


Yes.

### DMARC Usage

Does your company publish a signing policy using Domain-based Message Authentication, Reporting & Conformance (DMARC)?

986 respondents



Yes.

### Ensure Your Authentication Is Set Up Correctly

In an analysis of 1.5 million emails tested via Litmus Spam Testing, 28% showed issues with their DKIM records. Do your emails have authentication problems that you're not aware of? Litmus Spam Testing checks if your email is being properly authenticated using DKIM and SPF, and ensures that your DMARC record is set up correctly. If it's not, Spam Testing alerts you to exactly what's wrong and directs you on how to fix it.

[Activate your Litmus free trial coupon](#)

Try Spam Testing through this special [free trial offer](#).





# List-Unsubscribe & Encryption Usage

List-unsubscribe helps your deliverability by enabling inbox providers to provide an unsubscribe link that's native to their interface. This more prominent—and in many cases, more trusted—unsubscribe link prevents subscribers from casually using the Report Spam button to opt out, which harms senders' reputations.

List-unsubscribe has near-universal adoption, so brands that *don't* enable it stand out. Brands that have been blacklisted one or more times during the past year were significantly less likely than brands that hadn't been blacklisted to enable list-unsubscribe (91.4% vs. 96.4%).

Encryption is an emerging consideration made more important by high-profile cyberattacks and hackings. Gmail currently flags emails not encrypted with [Transport Layer Security \(TLS\)](#), so it's becoming a trust factor. It doesn't outright affect deliverability yet, but if more inbox providers follow Gmail's lead, then encryption could become an imperative.

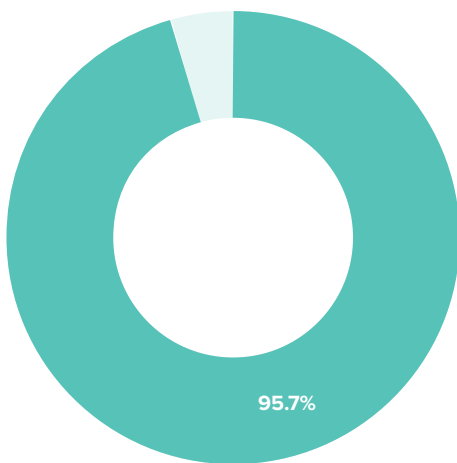
Marketers who describe their email programs as successful are 91% more likely than those at less successful programs to encrypt their emails (24.6% vs. 12.9%).

Some brands hesitate to give their subscribers another way to opt-out, especially when it's really prominent, as it is in the iPhone mail app. But here are [5 Reasons List-Unsubscribe Concerns Are Overblown](#).

### List-Unsubscribe Usage

Does your company enable list-unsubscribe functionality in their marketing emails?

1,989 respondents



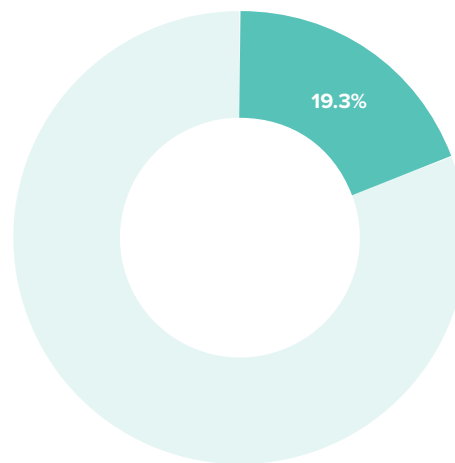
Yes.

Encryption was at the bottom of our list of [The Biggest Email Marketing Trends in 2017](#), but it could be a different story in 2018 if more inbox providers join Gmail in highlighting non-encrypted emails.

### Encryption Usage

Does your company encrypt your marketing emails using STARTTLS, Opportunistic TLS, or secure transport?

936 respondents



Yes.

### Are You Set Up for Inbox Success?

A faulty list-unsubscribe header can lead to avoidable spam complaints, and a lack of encryption in transit can open up your subscribers to breaches of privacy and spear phishing—especially if your emails contain a lot of personalized content. Litmus Spam Testing alerts you if your list-unsubscribe header isn't working correctly and if your email encryption isn't set up properly to protect your email content and subscribers.

Activate your Litmus free trial coupon

Try Spam Testing through this special [free trial offer](#).



# List Hygiene & Spam Filter Tools

Keeping email lists clean and emails out of spam filters is important and marketers have a number of tools to help them out. For instance, email address verification attempts to ensure that the addresses you're adding to your list are valid and deliverable. Marketers who describe their email programs as successful are 45% more likely than those at less successful programs to use an email address verification service (34.7% vs. 23.9%).

Bounce management services are another tool. The vast majority of marketers rely on their email service provider to remove email addresses that hard bounce to keep their invalid or unknown user rate as low as possible.

Allowing human discretion into the bounce management process appears to be risky. Brands that had been blacklisted one or more times during the past year were 26% more likely than brands that hadn't been blacklisted to manually handle hard bounces (19.2% vs. 15.3%). That makes sense, as marketers are surely always looking for reasons to keep an email address on their list.

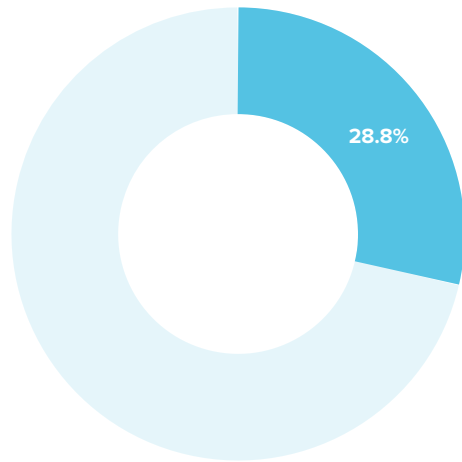
Spam filter testing tools are a third tool that can aid in deliverability. Successful email programs are 24% more likely than less successful programs to do spam filter testing (61.0% vs. 49.3%). Sophisticated programs use it at a similarly higher rate compared to less sophisticated programs (62.0% vs. 50.1%).



## Email Address Verification

Does your company use an email address verification service?

1,702 respondents



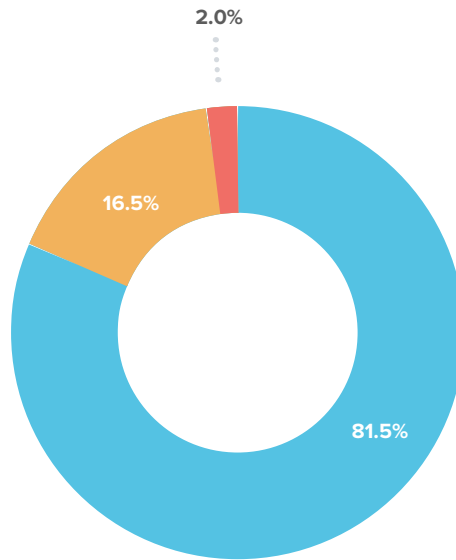
Yes.

BriteVerify and FreshAddress are the most popular email address verification services, with 35.4% and 14.6%, respectively, of respondents using those.

## Bounce Management

How does your company handle bounce management?

1,755 respondents



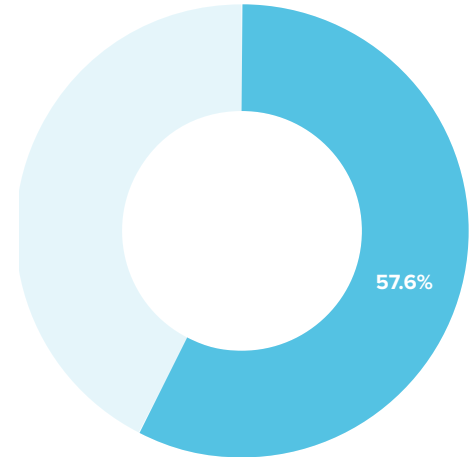
- Our email service provider handles bounces for us.
- We remove them manually.
- We use a 3rd-party solution.

When deciding on a bounce management strategy, make sure you understand the [difference between a hard and soft bounce](#).

## Spam Filter Testing Usage

Before sending an email, does your company run it through spam filter tests to identify potential problems?

1,865 respondents



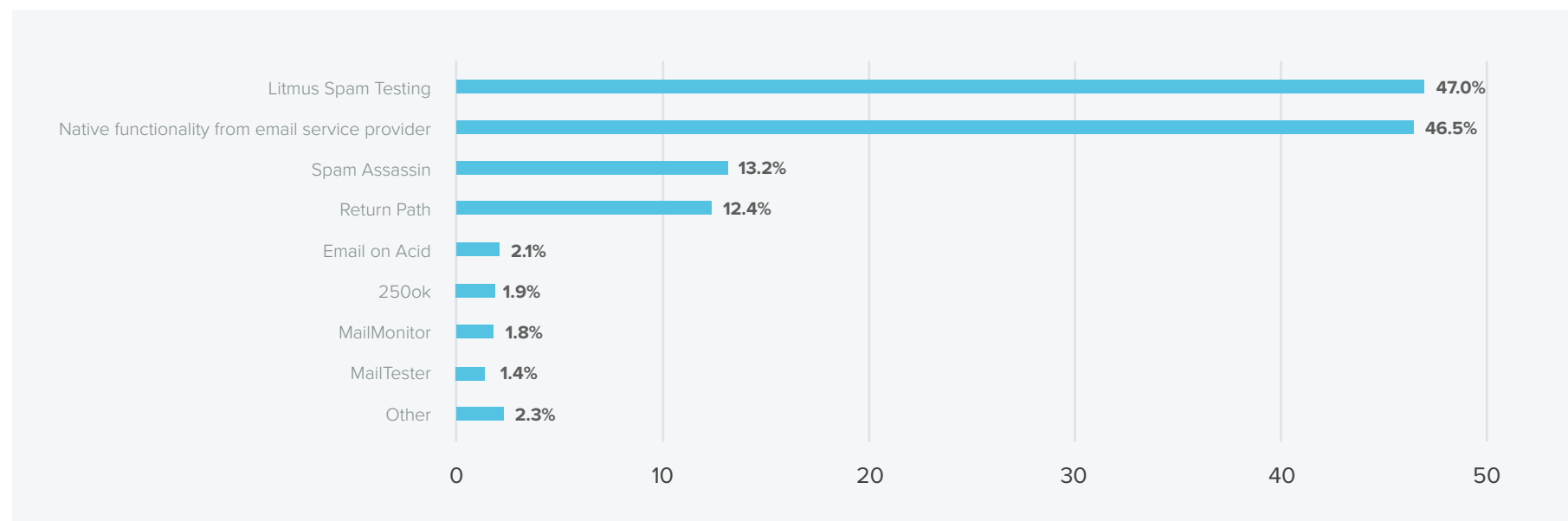
Yes.

Understand [why your content could be spammier than you think](#) and get your emails caught in spam filters.

# Spam Filters Used

What service or tool does your company use to check your emails against spam filters before you send them? (Select all that apply.)

980 respondents



Marketers use 1.3 spam filter tools on average. Of the marketers using two or more, 60.3% are using the spam filter tool provided by their ESP.

## Discover and Fix Spam Filter Problems

Litmus Spam Testing checks your emails against popular consumer and business-grade spam filters—including Gmail, Outlook, Barracuda, SpamAssassin, and many more—to alert you to issues before you hit send. Plus, we'll provide you with practical advice for how to fix issues and improve your email's chances of reaching the inbox.

[Activate your Litmus free trial coupon](#)

Try Spam Testing through this special [free trial offer](#).



# Inactivity Management

When subscribers stop engaging and customers stop converting, marketing automation can help, triggering re-engagement campaigns and win-back campaigns to get subscribers opening and clicking again and customers converting again, respectively.

Marketers who describe their programs as successful are 53% more likely than those at less successful programs to send re-engagement campaigns (55.5% vs. 36.2%). And marketers who describe their programs as successful are 60% more likely than those at less successful programs to send win-back campaigns (50.5% vs. 31.5%).

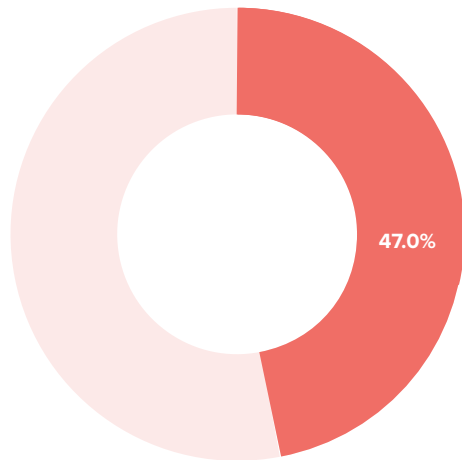
When re-engagement campaigns fail, brands then have to decide how to handle chronically inactive subscribers who haven't opened or clicked an email in a very long time. Successful programs are 24% more likely than less successful programs to eventually remove chronically inactive subscribers from their active mailing lists (59.0% vs. 47.6%).

Among brands that do remove inactives, most don't send a re-permission campaign that gives subscribers one last chance to indicate that they're still interested in receiving emails. Even among successful companies, only 45.7% have set up a re-permission campaign.

# Re-engagement Campaign Usage

Does your company trigger or send re-engagement campaigns to inactive subscribers?

1,706 respondents



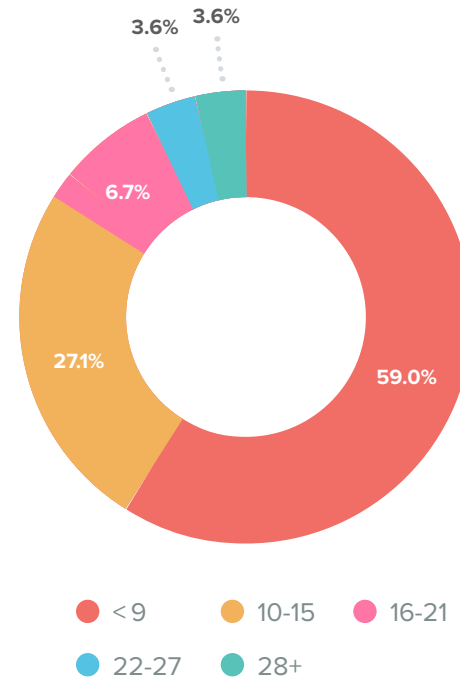
Yes.

52.3% of B2C brands use re-engagement campaigns, compared to 42.1% of B2B brands and 36.2% of nonprofits.

# Trigger for Re-engagement Campaigns

After how many months of subscriber inactivity does your company send re-engagement campaigns?

802 respondents



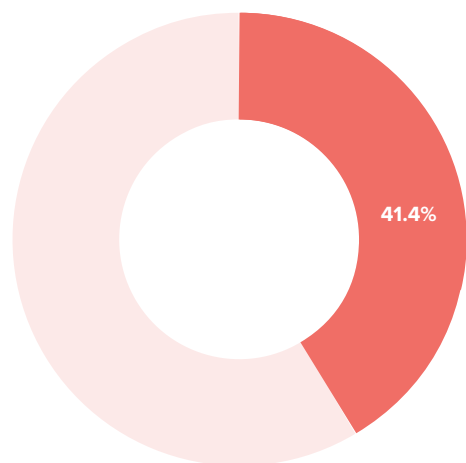
< 9 10-15 16-21 22-27 28+

Marketers who described their email program as successful are slightly more likely than those at less successful programs to send their re-engagement campaigns after 9 months or less of inactivity (60.6% vs. 56.2%).

# Win-Back Campaign Usage

Does your company trigger or send win-back campaigns to inactive customers who are subscribers?

1,625 respondents



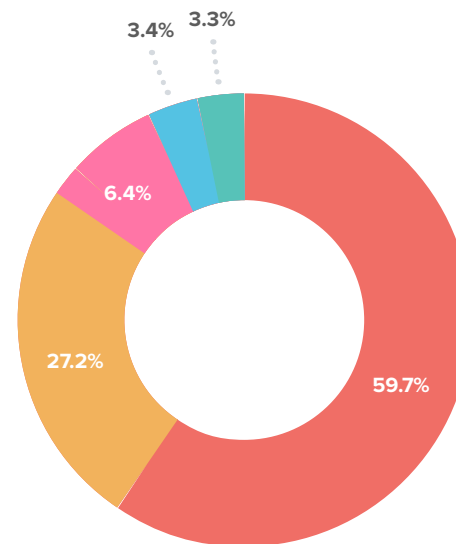
Yes.

B2C brands are 62% more likely than B2B brands to use win-back campaigns (52.1% vs. 32.2%).

# Trigger for Win-Back Campaigns

After how many months of customer inactivity does your company send win-back campaigns?

673 respondents



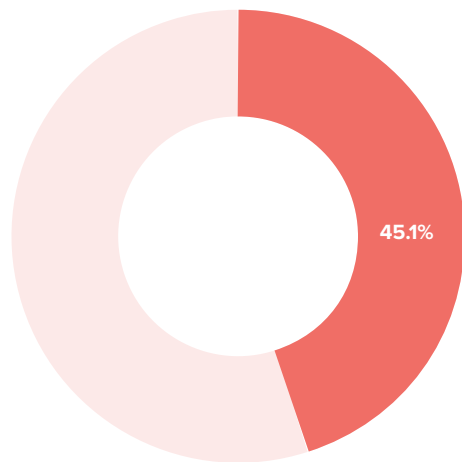
< 9 10-15 16-21  
22-27 28+

Win-back campaign users who described their email programs as successful are 17% more likely than those at less successful programs to send their win-back campaigns less than 9 months after a subscriber's last purchase (62.3% vs. 53.3%).

## Removing Chronically Inactive Subscribers

Does your company eventually remove chronically inactive subscribers from its active mailing list?

1,743 respondents



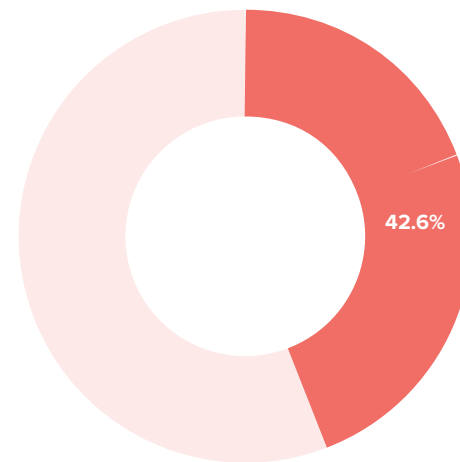
Yes.

Marketers who describe their email programs as successful are 24% more likely than those at less successful companies to remove chronically inactive subscribers from their active mailing lists (59.0% vs. 47.6%).

## Re-permission Campaign Usage

Does your company trigger or send re-permission campaigns to chronically inactive subscribers before removing them from its active mailing list?

814 respondents



Yes.

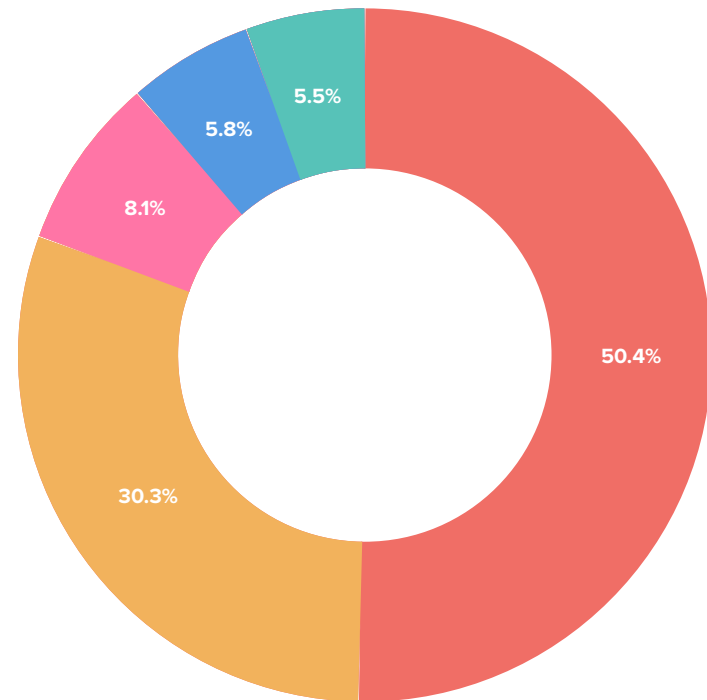
To be compliant with tough laws like CASL and GDPR, more brands are using re-permission campaigns. Learn [Everything You Need to Know About Canada's Anti-Spam Law in 2017](#) and [What GDPR, Europe's New Privacy Law, Means for Email Marketers](#).

## Trigger for Re-permission Campaigns

After how many months of subscriber inactivity does your company send re-permission campaigns?

347 respondents

When re-engagement campaigns fail, many brands move immediately to re-permission campaigns.



● < 9    ● 10-15    ● 16-21  
● 22-27    ● 28+

# Analytics & Deliverability Monitoring

Visibility enables success. For instance, marketers who describe their email programs as successful are 17% more likely than less successful programs to monitor their deliverability (84.9% vs. 72.7%).

While email service providers play a dominant role in giving their users both deliverability monitoring and performance analytics, our findings suggest that third-party solutions can give brands an edge.

For example, successful programs are 23% more likely than others to use additional analytics tools to supplement the performance dashboards provided by their email service provider (68.0% vs. 55.5%). Also, successful email programs are slightly less likely than less successful programs to use their ESP for deliverability monitoring (73.6% vs. 77.7%).

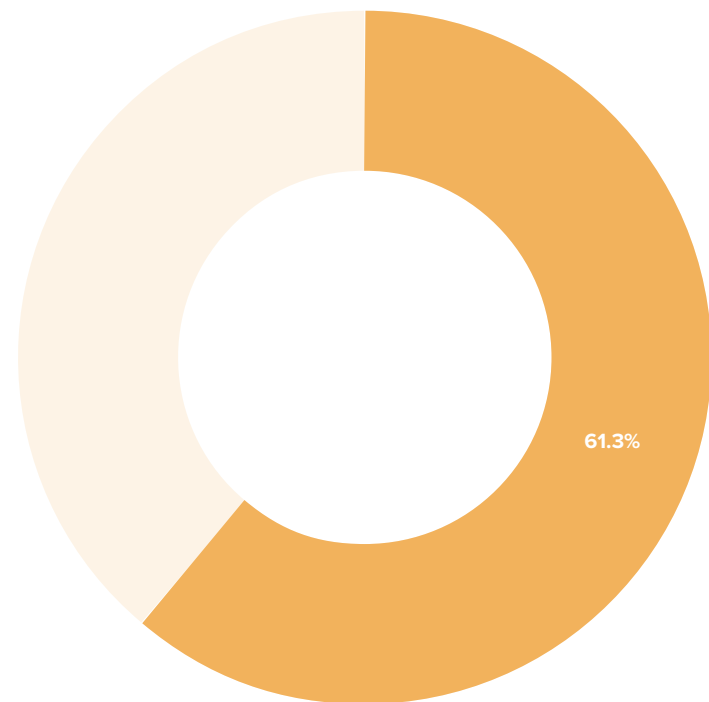


## Analytics Tools Used

Does your company use additional analytics tools to supplement the email metrics and performance dashboards provided by your email service provider?

1,880 respondents

Brands use 1.4 additional analytics tools to supplement their ESPs' analytics on average.



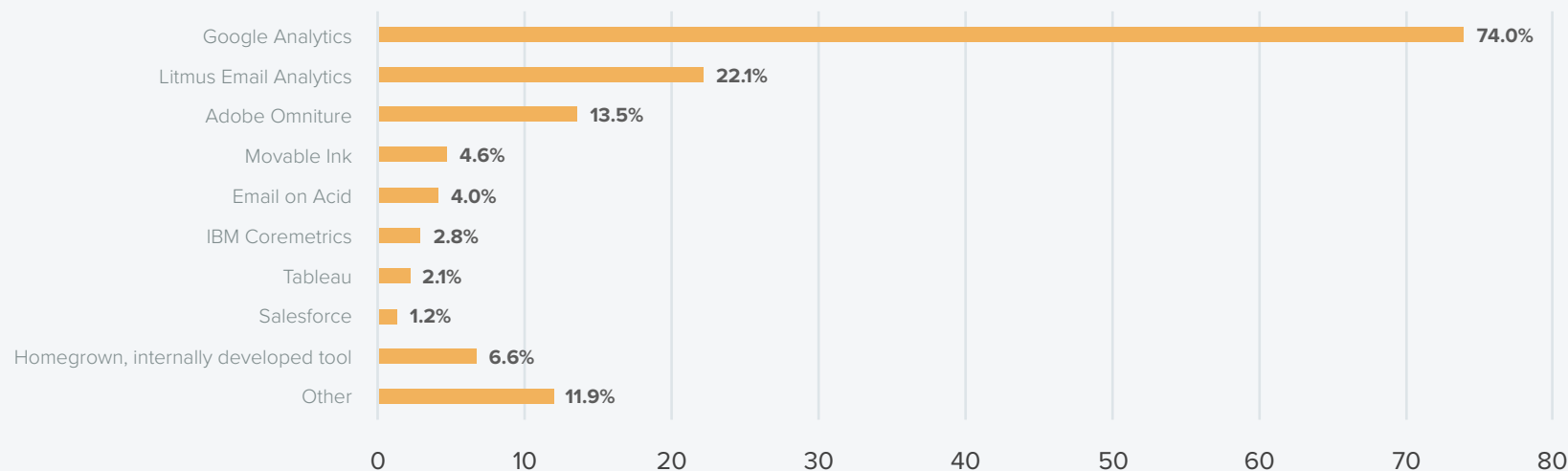
Yes.

# Supplemental Analytics

Which analytics tool(s) does your company use? (Select all that apply.)

1,063 respondents

70.1% of B2C brands use third-party analytics tools, compared to 54.7% of B2B brands and 53.4% of nonprofits.



## Go Beyond Opens and Clicks

Optimize your campaigns with subscriber-level insights to improve segmentation and targeting strategies. Litmus Email Analytics supplements the analytics provided by your email service provider, giving you additional insights into the email clients your subscribers use, how long they spend reading your emails, how many time they forward and print your emails, and more.

Activate your Litmus free trial coupon

Try Email Analytics through this special [free trial offer](#).

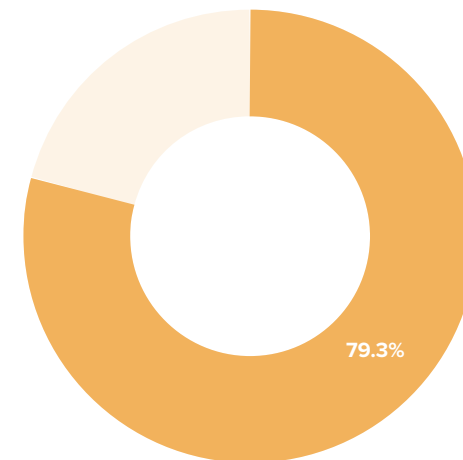


# Deliverability Monitoring

Does your company monitor its deliverability or inbox placement rate?

1,867 respondents

81.1% of B2C brands monitor their deliverability, compared to 78.9% of B2B brands and 71.7% of nonprofits.



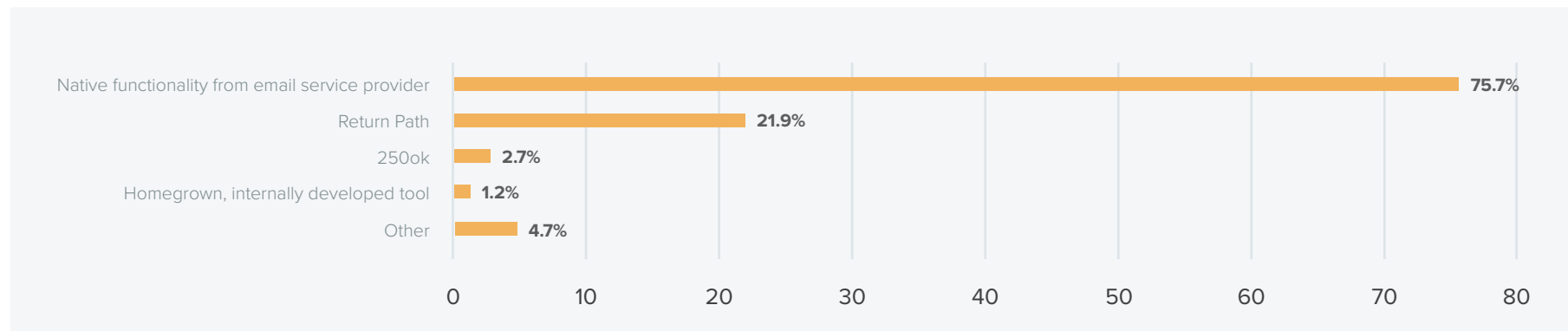
Yes.

# Deliverability Monitoring Tools Used

What service or tool does your company use to monitor its deliverability or inbox placement rate? (Select all that apply.)

1,249 respondents

Only 68.7% of B2C brands rely on ESP-provided deliverability monitoring, compared to 80.1% of B2B brands and 88.0% of nonprofits.



# Make it to the inbox, not the spam folder.

70% of emails show at least one issue that could impact deliverability. Ensure your email isn't one of them with Litmus Spam Testing.

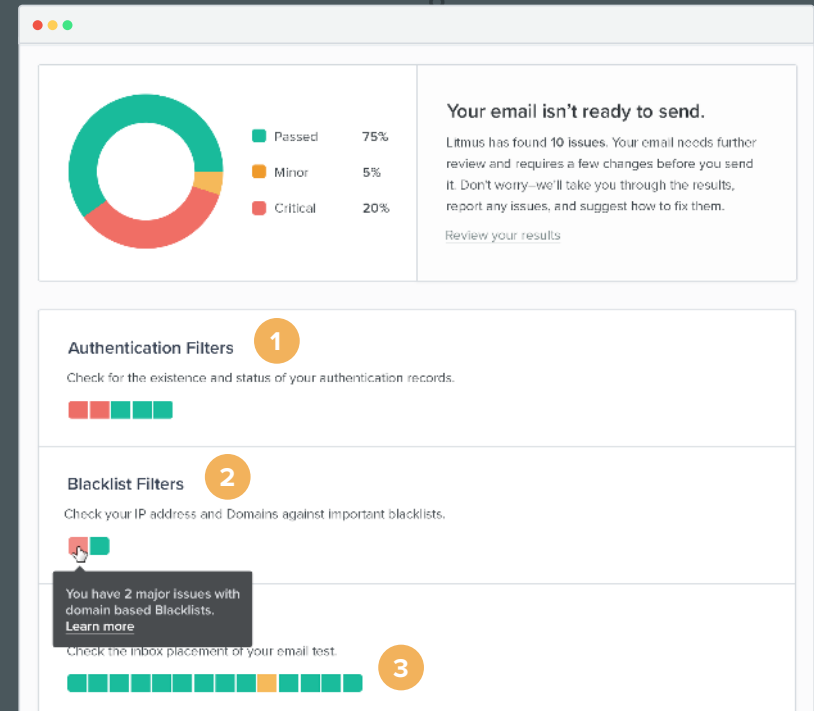
- **Fix issues that impact inbox placement**
- **Reach more subscribers**
- **Increase your email performance**

Litmus scans your emails against 27 different tests, identifies issues that might keep you from reaching the inbox, and provides actionable advice for how to fix them. Get the peace of mind that comes with knowing if your brand's emails are likely to reach the inbox.

- 1 Set your infrastructure up for success.** Validate that your email is being properly authenticated using DKIM and SPF, and ensure your DMARC record is set up correctly.
- 2 Know if you're blacklisted.** Check your IP addresses and domain names against common blacklists, and get notified if any of them could affect delivery.
- 3 Pre-screen your email across major spam filters.** Get your email scanned across spam filters from inbox providers and webmail services, as well as score-based filters that are frequently used for corporate spam filtering.
- 4 Get actionable advice.** Utilize hands-on, practical advice for how to fix issues and improve your email's chances of reaching the inbox.

Activate your Litmus free trial coupon

Try Spam Testing through this special [free trial offer](#).



The screenshot shows the Barracuda spam filter results table. The table has two columns: Status and Description Text. Each row represents a specific issue found by the filter, with a red 'X' icon in the Status column and a 'Get help' button in the Description Text column.

Status	Description Text
✗	You've used both dollar signs (\$) and exclamation marks (!) in the body of your email, this is considered spammy. <a href="#">Get help</a>
✗	You used the phrase "Dear (something)" within your email, this is very common in spam emails. <a href="#">Get help</a>
✗	You used the phrase "free" multiple times within your email, this is very common in spam emails. <a href="#">Get help</a>
✗	Your email has lots of images but relatively little text. Consider using fewer images and/or more text. <a href="#">Get help</a>
✗	The font's colour is very similar to that of the background. Avoid hiding words in your email. <a href="#">Get help</a>



## About Litmus

Major global brands across every industry and vertical trust Litmus to make email better, including 9 of the top 10 ecommerce brands, 7 of the top 10 technology companies, and 23 of the top 25 US ad agencies.

Backed by \$49M from Spectrum Equity, the Litmus email creation, testing, and analytics platform empowers marketers, designers, and agencies to confidently deliver customer experiences that ensure brand alignment and quality, as well as maximize performance and deliverability.

Headquartered in Cambridge, Mass., with additional offices in London and San Mateo, Calif., Litmus has partnered with more than 250 major email service providers and agencies, including MailChimp, IBM Watson Campaign Automation, and BrightWave Marketing. For more information about Litmus and the latest email news and trends, visit [www.litmus.com](http://www.litmus.com).



## About the Author

Chad White is the Research Director at Litmus and the author of *Email Marketing Rules* and thousands of posts and articles about email marketing. A former journalist at Condé Nast and Dow Jones & Co., he has spent more than a decade researching email trends and best practices at the Direct Marketing Association, Responsys, Salesforce.com, and in his current role.



## About the Designer

Andrea Smith is a freelance designer and abstract artist in Bluffton, SC with a passion for good software, travel, and rescue pups. With over twelve years of professional design and digital marketing experience, Andrea is an award-winning creative professional, recognized for strengths in strategic thinking, tactical planning, and design thought leadership.