HOW POLITICAL CAMPAIGNS CAN ENSURE THEIR EMAIL MESSAGES HIT HOME

By Len Shneyder
Vice President, Industry Relations, Twilio SendGrid
HOW POLITICAL CAMPAIGNS CAN ENSURE THEIR EMAIL MESSAGES HIT HOME

Executive Summary

The 2020 Presidential election is underway with one of the largest classes of candidates to ever run for the office at the same time. In a crowded field, communication to supporters and voters is critical to the viability of a campaign. Email is a crucial tool for reaching out to current and prospective supporters. Amidst such a crowded field and amongst so much activity, Twilio was curious as to the patterns of email outreach conducted by the presidential campaigns and how effective their emails were in terms of actually reaching their intended audience(s). As a result of our research and findings, we developed a set of recommendations for more effective email outreach by campaigns to recipients who have consented to receiving said emails from the campaign(s) of their choice.

- Only 3.8% of all the messages received landed in the primary tab of our test account. The primary tab in a Gmail account is the first thing a recipient sees upon opening Gmail in a web browser. Tabs help users separate out what is personal and direct (based on Google’s Algorithms, and that which is promotional or from social networks or spam). Default accounts in Gmail are created with a PRIMARY, SOCIAL, and PROMOTIONAL tab.

- 21.3% of all the messages our test account received landed in the spam folder, even though we had submitted our contact information and consented to receive emails. This is a major problem for campaign managers that are looking to make an impact in the inbox. The spam folder is associated with unsolicited commercial email and possibly abusive and deceptive messaging. Many users don’t check their spam folder—of further concern is that email from the spam folder is deleted on a 30 day rolling basis by default in Gmail, which means that messages could vanish altogether without ever having been seen.

- 74.8% of the messages received by our test account landed in the promotions folder. The promotions folder is meant to capture and store commercial and promotional content. Gmail’s algorithms determined that most of the political email messages sent by the campaigns should be sorted in the promotional tab. Although it may seem like the promotional tab is not where a campaign wants their email to land it is important to remember that tabs don’t exist on Apple mail and other native mobile email clients. Based on studies recipients do check the promotional tab but at a lower frequency than their primary tab.

- 38% of the campaign registration pages requested a phone number in addition to an email address. Of that 38%, only 30% (or 11% of the campaigns) sent an SMS message to the number we gave them. There are a number of reasons as to why we saw a lower frequency of SMS vs. email. SMS tends to have a higher cost on a per message basis vs. email; budget conscious campaigns need to invest their budgets carefully if they’re hoping to last throughout this incredibly long campaign season. Additionally, the number we registered with the campaigns simply could’ve been excluded by area code as
campaigns focus on battleground states. We expect to see SMS increase as we get closer to significant milestones such as registration, primaries and other events that will drive the need for more immediate notifications and responses.

- Almost 50% of campaigns either lacked a Domain Messaging Authentication Reporting and Conformance (DMARC) record or failed a DMARC check for their emails, thus leaving their brands and messages more open to spoofing and phishing attacks by not providing a set of instructions to the receiving domain e.g. Gmail, on what to do with spoofed email that fails authentication checks.

- Most candidates use multiple ‘friendly from’ addresses to make the recipient believe that someone other than the candidate is sending them an email. The friendly from address is the visible part of an email address often displayed in an email client as the person/entity sending the message. For example, the email address might include the familiar name of a celebrity, but it will still include @xxxforpresident.com.

- The average campaign employed 5.6 friendly from names but some went as high as 20 and some as few as one. Switching friendly from names appeared to be a way to grab recipients’ attention and convey different kinds of messages. The lack of consistency however may create uncertainty in the minds of recipients who will be faced with the question: “Do I know this sender and should I open the message?”

- Campaigns are not employing all the list hygiene practices they can to maintain a healthy database of email addresses. We saw large numbers of typo trap hits which indicate malformed email addresses and other data hygiene issues. Significant numbers of recycled trap hits were detected which can lead to blacklisting that can massively degrade a sender’s ability to deliver any mail.

- Campaigns leveraged up to four platforms to deliver email. Although diversification is admirable and helps spread the load, it can lead to unforeseen problems in terms of maintaining sender reputation and providing a consistent experience for recipients, not to mention managing and resolving deliverability issues when they arise.

- Most, if not all, candidates follow the news cycle and increase messaging based on current events. We saw large spikes in email traffic on the days leading up to events like the Democratic debates.
Introduction

The 2020 election has ushered forth what appears to be one of the largest gatherings of Democratic candidates running against an incumbent Republican president. The field, and ensuing news coverage, have created a massive test bed for capturing, measuring and evaluating political messaging across email and other channels. Over the past two to three presidential election cycles, candidates have realized that email is the most—if not one of the most cost effective mechanisms—for reaching a great majority of the electorate to facilitate distribution of their messaging platform and urge campaign donations.

However, the vast candidate field has had another less mentioned effect on the electorate: inbox and message over saturation. Candidates running for political office operate under a different set of guiding principles than brands and retailers that have been operating in the digital space for in some cases decades now. According to the Wall Street Journal, the more cringe worthy and sensational the subject lines the more effective the campaign. This advice often flies in the face of what legitimate brands and email marketers adopt as their MO to establishing a long term relationship with recipients. On the other hand, political candidates have a short amount of time to facilitate fund-raising, make their case to the electorate and ensure that they are at the top of the recipient’s inbox every day, all day and in lock step with the 24-hour news cycle.

Email marketing has been referred to as trench warfare. Brands vie for top placement, meaning they want their message at the top of a recipient’s inbox to improve their chances that the recipient will open the email, read it and take the prescribed action. Nowhere is this more true than with political campaigns where the need to drive recipients to donate could mean the difference between meeting goals and being included in highly visible debates or simply closing shop. The trench warfare often results in a constant stream of messages. The more sophisticated campaigns can do this across multiple communication channels.

When we started this research, the general election was still over a year away. We were fortunate in that none of the major candidates had, at that time, dropped out of the race. By the time this report will be published at least eight candidates will have dropped their bids. We posited at the start that cost would partially determine where we see the most messages. Email is the most cost effective channel, and often yields the highest return: $38 for every $1 of investment according to the Data and Marketing Association of the UK and more recently, Litmus measured the rate of return on email marketing at $42 for every $1 of investment. We theorized that political campaigns would lean heavily on email while SMS would be light given that it generally costs the sender more on a cost per message (CPM) basis. Based on pricing on Twilio’s own website, 1,000,000 SMS messages will cost $7,500 per month while the same number of emails will cost $399.95 per month before other considerations. To be fair, most campaigns will send well in excess of a million messages so there are volume discounts that will kick in, but a direct comparison demonstrates the basic concept that email is a highly cost effective means of reaching a large audience.

Based on Twilio’s Consumer Engagement Best Practices, email is still the most popular way for businesses to communicate with consumers. This stands to reason that political campaigns fall into the business communication category, which is partially defined as one-to-many communications and not person-to-person.
In general, what digital communication methods or channels do you prefer when receiving communications from businesses?

The same study discovered that TEXT/SMS was the most popular channel for urgent communications or those that require an immediate response. This seems to hold with our theory that TEXT/SMS will become a bigger component of political campaign messaging as the urgency mounts, such as when election day draws nearer and campaigns focus on driving voter turnout and the lifeline of donations ahead of major events.
The influence of email on voter turnout cannot be underestimated. Voters who are 60 years of age or older consistently rank as the highest performing age group. Furthermore, 85% of people who are 64 years or older use email, making the channel an ideal way to reach older votes who are twice as likely to cast votes based on data measuring the older vs. younger voter turnout.
Methodology

Subscription

In July 2019, we subscribed to every single Democratic candidate that had entered the race as defined by the New York Times “Who’s Running for President in 2020” interactive web page. We used this as a source of truth to ensure we did not leave anyone behind and to avoid making arbitrary decisions about which campaign/candidate to track. Additionally, we subscribed to the reelection campaign of the incumbent President. Finally, by subscribing to the emails, we were providing our consent to receive communications from the campaigns, emulating the real world experience of other recipients. As such, our results—and recommendations—reflect wanted communications, as opposed to unwanted, spammed email.

During the subscription process we offered the campaigns every piece of information that their registration pages requested. If a campaign asked for a zip code in the San Francisco Bay Area, we provided one, and used that same consistent zip code across all campaign registration pages. If a campaign requested a phone number, we provided a 510 area code number for tracking any SMS messages that campaign sent during our tracking period.

Why We Used A Gmail Account

We chose to use a single, newly created, Gmail account to receive all of the messages. We did not mark any messages as spam, nor did we open any of the messages or do anything other than catalogue them during our tracking period to avoid predisposing the account to user behaviors that could affect the final disposition of messages it received. We chose Gmail because it is the largest single free mailbox provider on the planet with more than 1.4 billion active users based on 2018 stats.

Free mailbox providers have long since eclipsed other email providers in terms of mailboxes and usage. When people move residences they may be forced to change their ISP. Using Gmail, Outlook.com or any of the other free mailbox providers allows users to keep their email address and the contents of their inbox undisturbed. There are other reasons why webmail providers have grown, including consolidation of smaller domains, investment in the UI and unique tools to bring greater utility to email. The most recent innovations include Google’s AMP for Email which is bringing interactivity to the inbox and turning into a more engaging channel.

Window of Observation

We tracked all communications to the single Gmail address we enrolled for a period of 30 days in addition to any and all SMS messages campaigns sent during those 30 same days. We checked our Gmail account’s promotions tab, primary tab and junk tab on a daily basis and logged where messages landed and the kinds of from addresses employed. We then evaluated the underlying sending architecture, platforms and mechanisms that were used to deliver the emails in order to determine if the candidates and campaigns were employing best common messaging practices.
HOW POLITICAL CAMPAIGNS ENSURE THEIR EMAIL MESSAGES HIT HOME

Message Placement

Message placement is crucial to improving the likelihood of someone opening and reading the email, and then acting on the call to action.

Although most brands—and campaign strategists for that matter—would ideally like to see their messages land in the primary tab, the messages themselves are actually more promotional in nature and thus belong in the promotional tab based on Gmail’s logic. Things to keep in mind about message placement: mobile devices not using Google’s inbox app have no concept of tabs. A message received in the promotional tab will display as ‘inbox’ in a native iOS mail application. The only place where tab placement is relevant is in Google products on mobile devices and browser based viewing of email through gmail. Any messages that are i-mapped into a desktop email client such as Apple mail or Thunderbird will likewise not respect tabs as a means of organizing and displaying mail. Still, given the popularity of Gmail among users it is important to note that tab placement is relevant to some portion of the population. However, based on research from Return Path, 90% of users felt tabs correctly categorized received messages. More importantly less than 20% of users never check the tabs demonstrating that most users will at some point check the messages in the tabs.

Email marketing benchmarks routinely measure the percentage of email that winds up in the spam folder or is blocked. Based on metrics released over the years from companies such as 250ok, Return Path and eData Source, 20% of commercial messages never reach the inbox. Since we don’t have the ability to measure the percent of blocked messages, we look to the percent that winds up in the spam folder as a measure of overall efficacy. More than 21% of all messages we tracked wound up in the spam folder. Of the 26 candidates we tracked, two of them -- or 7% of the field -- never delivered email to anything but the spam folder. Most candidates’ email wound up in the promotional tab and only a minority ever reached the primary tab.
Frequency

The question of frequency has been the subject of countless articles, blog posts, tweets and webinars among email marketers, not to mention entire technologies dedicated to determining how often to deliver email to a given recipient, segment or demographic. Questions such as how many messages are too many before a recipient becomes unengaged remain top of mind for email marketers as they test the frequency and cadence of campaigns while scaling their efforts through automation, triggers and other unique methods to ensure brand stickiness and user engagement leading to conversion.

Political campaigns are incredibly different given their temporary if not fleeting existence. Political campaigns must achieve goals much faster than retailers or else suffer the consequences of not only becoming quickly obsolete and dismissed, but running out of funding to keep the lights on.

Message frequency reached a fever pitch on July 31st, the second day of the two day Democratic debate. Our test account received 60 messages that day across all placements. This means that we received almost three messages per campaign that day urging voters to watch the debates, donate and any other number of calls to action.

It’s worth mentioning that during our tracking, three of the campaigns never sent an email and as such we’re really only dealing with 23 active of the total 26 tracked. Daily volumes ranged from 11 to 60 messages showing vastly different campaign messaging tactics and approaches. As mentioned earlier, messaging often followed the news cycle and was reflected in the content of the emails as well as their frequency and urgency. The peak on July 23rd can be tied to the Mueller testimony on Capitol Hill.
On average, each campaign sent 1.5 emails per day, but it was not uncommon for a single campaign to send four or even five emails in a single day! About 50% of the campaigns delivered email on a daily basis, thereby remaining a fixture of every recipient’s daily inbox experience. Based on Twilio’s Consumer Engagement Best Practices, older consumers wish to be contacted about once a week at a lower rate than younger consumers for promotional purposes. Promoting candidates, their platforms and soliciting donations for a campaign would all fit in the category of promotions. Baby Boomers having a higher propensity to vote in elections should be taken into account when campaigns design their campaign websites. Not a single one of the candidates we reviewed offered the option to set the frequency and cadence of communications. It was all or nothing across the board.
There was no clear correlation between sending frequency and message disposition. Campaigns that sent higher volumes of email over the course of our 30 days did not wind up performing worse in terms of message placement than those that sent less frequently. Most email marketers set and establish a regular cadence as an important step to establishing a good sending reputation. New sending IPs and domains need to be warmed over time to yield the best results.
Friendly From Names

Most email marketers believe that brand consistency is key to helping recipients differentiate between competitors. Deliverability experts often advise senders that establishing and maintaining a consistent brand is key to helping recipients differentiate legitimate mail from fraud. The advice most of these experts give to brands and email marketers is to choose an email address and stick with it. A further refinement of that message would be to choose a friendly from name (this is the part of the address that’s commonly displayed in an email client, e.g. Brand X vs. email@communication.brandx.com) and ensure that it’s visible and consistent. What that means in practical terms is that the friendly from isn’t so long as to be clipped, is not a call to action in and of itself, clearly identifies the sender and or brand and is as uniform as possible.

We can confidently say that this best practice is not followed at all by political campaigns. On average, we saw 5.7 friendly from addresses per campaign. One campaign had 20 different friendly from addresses in operation over the 30 days of tracking. Double digit numbers of friendly from addresses were not uncommon. With only one exception the underlying from addresses were consistent. Often times the same strategy was employed by campaigns to create different friendly from addresses. Some of these variations include, but are not limited to:

- First Name Last Name
- First Name 2020
- First Name Last Name 2020
- First Name Last Name HQ
- FirstNameLastName.com
- Team Last Name
- Spouse’s First Name Last Name

Often times campaigns would send emails in the name of their campaign manager. Some campaigns sent emails using the name of a well known public figure who was messaging the voter on behalf of the campaign.

Not all of the varied uses of campaign names were above board. At times some of the campaign names included things like [BREAKING News], URGENT, multiple punctuation marks and other tactics associated with spammers created to grab the attention of the recipient no matter what the relevance of the content.

Most campaigns realize that identifying the sender, and making it obvious in the list view, is critical to helping the voter establish the message sender’s identity and relevance before opening the message. The use of so many varied and at times clipped from names creates uncertainty and possibly leads to numerous messages being deleted without opening them. In an era where both politicians, their campaigns, brands, financial institutions and any other well known entity is fodder for phishers and cyber criminals to impersonate, creating consistent brand and name recognition for recipients is key in creating an authentic and reliable experience.
Subject Lines

Not to be overlooked, subject lines are crucial in establishing the reason why a person should, or should not, open a given email. Subject lines can take numerous forms—similarly there are numerous kinds of subject lines that should never be sent. The length, tone and call to action contained in subject lines are tested and refined by email marketers the world over. Artificial intelligence and highly structured testing schemas have evolved in the marketplace to craft the perfect subject line. According to Convince&Convert, 35% of recipients open emails based on the subject line alone!

During our study we saw every manor of subject line that used every trick and subterfuge to compel the recipient to open. From making ‘personal requests’ to sensationalizing the subject line through BREAKING NEWS ALERTS, punctuation marks, emojis and subject lines that well exceed any accepted standards or lengths and will surely be clipped by mobile email clients, and in some cases, web clients:

“We’re launching a new goal: to receive two million contributions from our grassroots supporters.”

The preceding subject line taken from a campaign is 96 characters in length or 14 words. The average iPhone users sees about 35-38 characters of a subject line in portrait mode. It should come as no surprise that more than 40% of all email is opened on a mobile device. Some would put that number much higher among certain demographics. Still, since less and less people are opening email on their desktop or laptop, not accounting for the email experience on an iPhone is clearly a miss.

In 2017, Twilio SendGrid analyzed billions of emails sent on Black Friday and Cyber Monday, the highest single days for email marketing. We discovered that seven word subject lines were the most popular in English language emails. However, it was the use of four word subject lines that correlated with higher engagement and open rates. This held true in 2018 with seven and eight word subject lines being popular; however, engagement remained tied to shorter and pithier statements. This analysis would seem to agree with Marketo’s analysis of 41 characters as an optimal length in 2019 which is 10 characters shorter than the previous year.

You’ve helped me get back on my growth trajectory, friend. I’m not going to ask less of you, but more of...
[the subject line above was clipped by the webmail client]

You’ve helped me get back on my growth trajectory, friend. I’m not going to ask less of you, but more of you.
[the full subject line at 109 characters]

Campaigns employ emojis which we discovered in previous analysis to have limited impact on open and engagement rates. In some cases the emojis can be rather deceptive as in this instance where the use of a paperclip can imply an attachment where none is present:
Sending attachments as part of marketing communications is not considered a best practice—executable attachments are almost universally blocked by mailbox providers. Cyber criminals exploit file attachments routinely to infect receiving computers with malware through executables and macros hidden in seemingly innocuous PDFs and other file types. To be clear, we didn’t receive any attachments from any of the political campaigns.

Other peculiar subject lines include one word subject lines “hey” or “Bump” or “Lies” “you up?” “before bed” as if you know the candidate and they know you so they should be able to send you such informal messages.

Some, not all, of the campaigns we tracked took advantage of pre-headers. Subject lines are generally followed by a short snippet that can be controlled by the sender. The snippet can contain links, a common practice when the mobile web was in its infancy, urging the recipient to open the email in a browser for a better viewing experience. More commonly, today the pre-header works in concert with the subject line to craft a complete thought or a call to action. Both can be carried over to each medium so that a person using a mobile device and viewing as a list can read the subject line and pre-header can determine, at a glance, the purpose for the email and establish whether they want to open it or not. Campaigns that did not use a pre-header at all used just the subject line followed by as much of the first line of text that could be accommodated in the display line of the email. This could potentially create a confusing experience for a recipient because some of the subject lines are so disconnected from the purpose of the email as to be viewed as deceiving.

**Subject:**
We can flip this district:

**Visible Subject + Pre-header:**
We can flip this district: - In a district roiled by a major ballot fraud scandal, Dan McCready is hoping to filip Nort...

**1st full paragraph:**
We’re more than 15 months away from the presidential election. But in North Carolina, an important special election is just seven weeks away. In a district roiled by major ballot fraud scandal, Dan McCready is hoping to flip North Carolina’s 9th from red to blue.
From what we observed in our test account, political campaigns employ a shock and awe campaign strategy to compel recipients to open their messages. Not only are the people running the campaigns aware that they’re fighting for a limited set of donation dollars, but they’re also vying for limited attention spans that are split between competing campaigns and all the day-to-day business that happens in the inbox. There are no rules and there are no guidelines when it comes to what campaigns will or will not do to garner an open, followed by a click and a donation. In a digital world where nothing is as it seems, email marketing pundits have been preaching brand and messaging authenticity as crucial to being recognized and increasing engagement. Since every campaign, save for one, will be discarded, the idea of consistent authenticity through subject lines and messaging is tabled in favor of expediency and drawing the attention of recipients, at any cost.

Unfortunately, this is short-sighted. The language in the body of emails, subject lines and other characteristics are taken into consideration by mailbox providers when deciding on where to place a message. As we previously stated, we saw campaigns whose emails never delivered to anything but our spam folder. Sensational copy can be part of the reason why some of these emails never saw the light of the promotions tab. There are most likely more than one reason why this happened, but for campaign managers that believe there are no rules, or no guidelines to sending emails on behalf of campaigns, we would caution them to test and evaluate their copy as it may well be the culprit that is destroying their overall deliverability.

Authentication

When email was created in the early 1970s there was no such thing as phishing or spear phishing to take into account. Email was constructed as an open platform to connect the builders of what was then ARPANET and later the internet. Decades later, email connected the world’s population and by extension was abused because it was capable of reaching so many people.

Email authentication as we know it today started in the early 2000s with simple solutions to establish the authenticity of the sender while providing identifiers and policy for receiving domains to help them determine the best place to deliver a message: the inbox, spam folder or not at all. What started as a simple association of IP and domain has evolved to include cryptographic identifiers, forensic reporting and DNS based policy. Today there are three primary forms of email authentication:

- **Sender Policy Framework (SPF)** — This authorizes mail to be sent by a domain via a certain IP or set of IPs. This was also the first form of email authentication and is published as a text record in DNS.

- **Domain Keys Identified Mail (DKIM)** — DKIM is a cryptographic signature using a private/public key pair that attaches a unique identifier to a message and also allows a receiving domain to determine if the message body has been tampered with in transit, or if someone is spoofing part of the message to bypass a mailbox provider’s filtering. DKIM is integral to financial institutions that are highly phished and spoofed by bad actors.
• **Domain Messaging Authentication Reporting and Conformance (DMARC)** — This is the most recent form of email authentication that ties SPF and DKIM together via a policy that is published in DNS and instructs the receiving domain operator or mailbox provider with what to do if a message fails an SPF check, a DKIM check or both. The policy can be constructed as to allow the delivery regardless of failure, or not deliver the messages, thus preventing potentially fraudulent messages from entering the inbox of unsuspecting recipients. An added benefit of DMARC is the ability to receive forensic reports from mailbox providers to better understand who may be attempting to spoof your brand.

Although DMARC has been available for more than five years, its implementation has been slow among the private sector. In 2017 the Department of Homeland Security issued Binding Operational Directive 18-01 to enhance web and email security that required all government domains sending email to employ DMARC, and thereby necessitating SPF and DKIM. The U.S. government is more secure now, in terms of its email communications, than the private sector in the United States.

• We looked at messages from each campaign to determine if they were using any forms of email authentication

• Fewer than 50% of the campaigns employed and passed email authentication checks.

• 42% of the campaigns had either a missing DMARC record or were failing a DMARC check.

• 100% of the campaigns we tracked published an SPF record

• 100% of the campaigns we tracked published a DKIM record but 9%, or 2, had a DKIM record that failed verification.

The presence or absence of these records did not seem to have a correlating effect on message disposition. Mailbox providers such as Gmail necessarily block or deliver messages on the absence or presence of email authentication—it is a strong data point in the overall reputation logic and helps them make informed decisions on delivery. However, as email marketers in the private sector have learned, employing email authentication as part of an organization’s email sending architecture has several benefits:

1. Protecting the brand by making it more difficult for bad actors to spoof the sending domain

2. Protecting recipients by decreasing the ability of bad actors to spoof the brand’s domain and thereby trick them into disclosing personally identifiable information (PII)

3. Mailbox providers will have an additional data point that will help differentiate the sender’s message stream from that of bad actors thereby building a positive sending reputation and improved deliverability

It is not uncommon for bad actors to sign email authentication records on fraudulent domains that they create to try and bypass mailbox provider filters. Email authentication is but one data point in a complex construct that are the front-line defenses of the world’s leading mailbox providers. However, email
authentication is a crucial tool in the battle against phishing and should be employed by every entity wishing to send email on the internet. The bigger the entity the bigger a target they are for cyber criminals because they will naturally have better email sending reputations and thus by extension larger populations of recipients willing to take prescribed actions. Given a political campaign’s reach, and the importance placed on their messages, the compressed time frame to get that message out, the potentially massive effect they can have on the very fabric of our country, and the unprecedented activity of foreign interference in the previous and upcoming election, every single one should be signed and pass all three authentication checks.

**Spam Traps**

Email marketers have long been leery of spam traps and their deleterious effects on the deliverability of a given campaign. On the flip side, mailbox providers and blacklist operators have long employed spam traps as a means to gauge the legitimacy of a sender, catch bad actors and apply the data as part of establishing sending reputations. There are three primary flavors of spam traps and each tell a different story about the sender:

1. **Recycled Spam Traps**—These email addresses at one time received email but the recipient shut down the address, stopped using it etc. Sometimes these traps are referred to as honeypots. Mailbox providers will often turn these addresses off for a period of time, sometimes for years, and issue a hard bounce so that they can be removed from a given sender that is complying with best practices. After a period of time they will turn the address back on to see what lands in the mailbox.

2. **Typo Spam Traps**—One of the more difficult problems to solve in email is the proliferation of look alike or cousin domains. These are domains that look like legitimate domains e.g. hotmall.com vs. hotmail.com or g00gle.com vs. google.com. Typo traps are meant to identify senders who have poor list hygiene practices when collecting email addresses.

3. **Pristine Spam Traps**—This kind of spam trap is often used to catch people who screen scrape websites for email addresses or obtain them through other illicit means.

We saw anywhere from 30%-55% of the traps the campaigns hit as Typo traps indicating poor list hygiene and a reluctance to give up addresses that may be malformed or tied to now defunct domains and ISPs. In some cases campaigns had double digits of pristine traps which could signal a much deeper problem: where the data came from, if they were relying on a third party data provider rather than growing their lists organically, and other even more troubling issues.

Spam traps are a reality when it comes to email. Not all traps networks are maintained by mailbox providers. Some are operated by independent third party operators such as Spamhaus that have been operating and monitoring these traps as part of their effort to curb abuse of the messaging ecosystem. [Spamhaus](https://www.spamhaus.org) publishes different kinds of blacklists based on the severity of hits to their trap networks as a means
of stopping mail flow from abusive IPs, domains and the very real and ongoing threat of botnet attacks which are characterized by a large volume of email spread across a wide range of sending IPs and domains and sent in small quantities making it incredibly difficult to stop.

Not all blacklists are alike. Spamhaus is the largest and most legitimate black list operator, which is why their lists are employed by numerous domains and entities around the world. When a sender is on a Spamhaus blacklist the effect is significant: a large portion of email will be rejected because the sending IPs have been blacklisted. On the other hand, there are other operators that essentially charge for removal, something Spamhaus never does, and their market penetration is much smaller. Other blacklists are altogether unreasonable and employed by very few domains who have no real impact when a sender’s IP winds up one of them.

**TIP:** Being blacklisted can represent a significant challenge to a political campaign or business. As important as it is to remediate the listing by understanding the requirements for delisting, it is equally important to understand why the listing happened in the first place. Problems leading to a listing that aren’t analyzed and resolved will simply result in further listings which will become more difficult to resolve through repeated abuse. More information on how to avoid being blacklisted can be found on Twilio SendGrid’s blog.

**Platform**

Sending email at scale is no easy task, hence the proliferation and specialization of email platforms that cater to unique segments of the market. Numerous campaigns used more than one platform to send email. In some cases we saw as many as four platforms employed in sending emails, thus spreading the brand across multiple architectures, possibly domains, and compounding the problems that a campaign will have to deal with in order to achieve maximum deliverability and inbox placement.

By and large the campaigns used one of only a handful of platforms for the bulk of their email:

- Actionkit
- Acoustic
- Blue State Digital
- NGP VAN
- Mailchimp
- Salsa Labs
- Twilio SendGrid

In some cases, we saw whole mailstreams switch from one provider to another over a period of time. In other cases, two or more of the platforms mentioned above were used, and in other cases it wasn’t possible to identify the platform being used.
Multi-platform deployment may seem like a good idea because it spreads the load and dilutes complaints and messages marked as spam, but email authentication and the need for consistency ties it all back together. Entities sending email across too many IP addresses or through too many providers may begin to look like spammers conducting what’s called a snow-shoe attack. Snow-shoe attacks are characterized by smaller volumes of email spread across large swaths of IPs to hide the true nature of the delivery and make it more difficult to stop. Although not the intention of a political campaign, by using numerous platforms, different networks of IPs, different sending architectures, and then hoping to tie it all together with accurate email authentication records, all of it increases the complexity of the endeavor and creates more opportunity for user error. Given the relatively short shelf life of political campaigns, the need to get to market quickly may encourage the campaigns marketers to cut corners in an attempt to ensure their message is reaching the inboxes of the voting public. However, unless campaigns focus on sending email in a manner that conforms to accepted sending best practices, they run the risk of shutting themselves out of the inbox and limiting their ability to fundraise and discuss their platforms and policies.

Multi-Channel

We theorized that we wouldn’t see as much SMS because, as we stated in the introduction, email is more cost effective. However, SMS will certainly be a feature as we approach key milestones like the Iowa caucuses and New Hampshire primaries, but at this early juncture it is the purview of large war chests only. Only 35% of the campaigns asked for a phone number when we signed up to receive their emails. Where a phone number was requested, we gave the campaign a consistent phone number to track SMS that were sent to the number. Of the 35%, three campaign sites actually had an explicit opt-in for SMS. One of the campaigns pre-checked the opt-in box while the other two did not. We call this out because pre-checked boxes are prohibited under the General Data Protection Regulation, (GDPR). We realize this is the US election but we believe that good privacy standards start by complying with the strictest regimes. It’s also important to keep in mind that GDPR covers anyone (regardless of nationality) who lives within the EU, thus a pre-checked box for an American ex-pat wishing to vote in the US election could theoretically be a violation under GDPR.

Only 12%, or three campaigns, actually sent SMS messages during the period that we tracked the campaigns’ messaging activity. With only two exceptions, the campaigns sent one message per day with no regular cadence. The two exceptions featured two messages on two separate occasions. The SMS were mostly tied to the news cycle or reinforced a given message from a specific candidate. We captured 22 messages during our study, a small fraction of what we expect to see as we get closer to significant milestones.

SMS has been an important feature of political messaging dating back to the 2014 midterms. Texting has a 98 percent read rate and gets six to eight times the response rate of emails, according to campaign consultants. Texts get twice the response of phone-banking calls to mobile numbers, and 36 times the response that emails do. The cost to send a text message can be as little as 6 cents, while a direct mailer
costs as much as 65 cents, political consultants say. However, as stated before, campaigns must decide where their limited funds are best spent. Given the amount of time before the first primary elections, it makes sense for campaigns to focus their dollars on email to vye for the attention of the voting public. SMS will be saved for more critical moments where they will demand the voters’ involvement to either donate or ensure voters are getting to the polls ahead of primary elections and the general election.

Best Practices

After reviewing sample messages across more than 20 campaigns and evaluating how those messages were sent, along with the frequency and timing of those messages, we’ve concluded there are a basic set of key recommendations that all campaign managers charged with scaling email communications on behalf of candidates should follow.

1. **Consistency**

Consistency has always been a requirement for businesses wanting to leverage and grow email communications. Deliverability experts have often advised senders to send more frequently but at slightly decreased volumes versus large deliveries unevenly distributed throughout the week or month. Consistency is key to establishing and building a positive sending reputation. But consistent volume is only the tip of the iceberg. One of the ways political campaigns can create consistency is to:

- Limit the number of friendly from names and stick to whatever the subset of those from names are. Think of each “from” name as a different call to action or a sub brand of the campaign. Merchandise could live under one friendly from, the candidates direct voice under another, news under a third. This is not a hard and fast rule but having too many friendly from names creates uncertainty where there should be clarity and confidence.

- Another application of the consistency rule is in terms of frequency in cadence. Political campaigns have a unique opportunity to set cadence as a preference, configurable by the subscriber, at the time of subscription. Some voters may want all of the communications while others are happy with a weekly digest. Giving people the power to determine their level of comfort will breed higher levels of engagement and avoid list churn and recipient burn out.

2. **Hygiene**

The need to get the candidate’s message out to as broad a population as possible must be tempered with an understanding that not every email address in the database should receive a communication. Appropriate hygiene controls should be applied. Those could include using validation tools to check for malformed addresses, ferreting out known hard bounces and avoiding delivering email to role accounts and known ‘dead’ domains because they may be trap networks. Because campaigns are collecting addresses from people at a multitude of in-person events, extra care needs to be applied to how those address-
es enter the mailable database. The effect of hard bounces, spam trap hits and overall bad list hygiene will result in a smaller footprint for email campaigns because they will wind up in the spam folder or be blocked out right.

3. **Authentication**

The internet is not only the information superhighway that's shrunk the world and connected some of its most remote corners, but is simultaneously a shroud for the worst forms of information and identity theft imaginable. In the United States, the political campaign season has become nearly endless as evidenced by the Trump campaign who set up their reelection bid during the first months of the administration. This campaign season effectively started after the midterm elections making it a long process. Given the length of the campaign season, the need for fundraising can't be overstated. Protecting a campaign's communications through the careful application of email authentication at enforcement will not only prevent bad actors from capitalizing on a candidate's success and reach, but it'll make the mailboxes of millions of Americans a safer place for the democratic process to unfold.

---

**About Twilio**

Millions of developers around the world have used Twilio to unlock the magic of communications to improve any human experience. Twilio has democratized communications channels like voice, text, chat, video and email by virtualizing the world’s communications infrastructure through APIs that are simple enough for any developer to use, yet robust enough to power the world’s most demanding applications. By making communications a part of every software developer’s toolkit, Twilio is enabling innovators across every industry—from emerging leaders to the world’s largest organizations—to reinvent how companies engage with their customers.