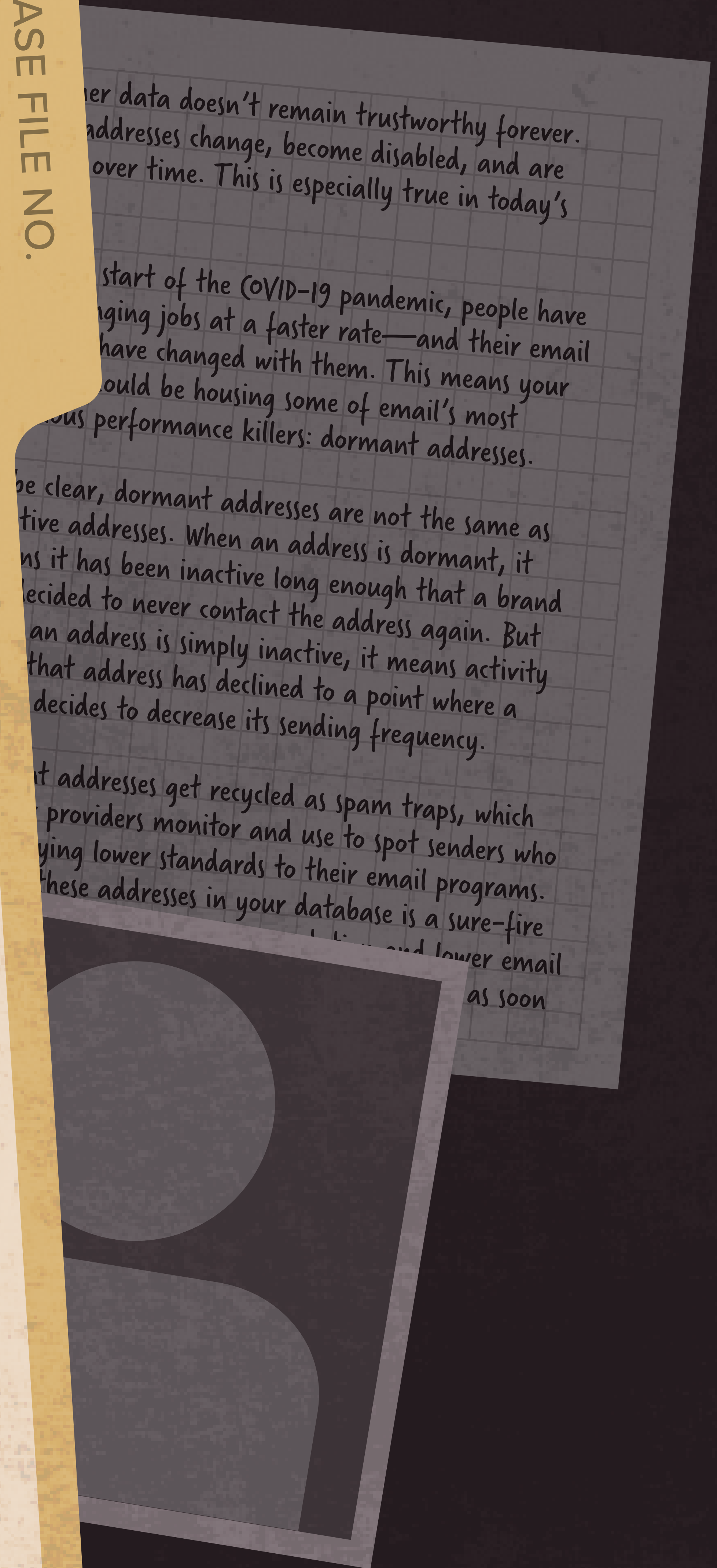
Clueing in on List Hygiene

CATCH THE CULPRIT OF POOR EMAIL PERFORMANCE

validity

IMPORTANT

CASE FILE NO.
05292022

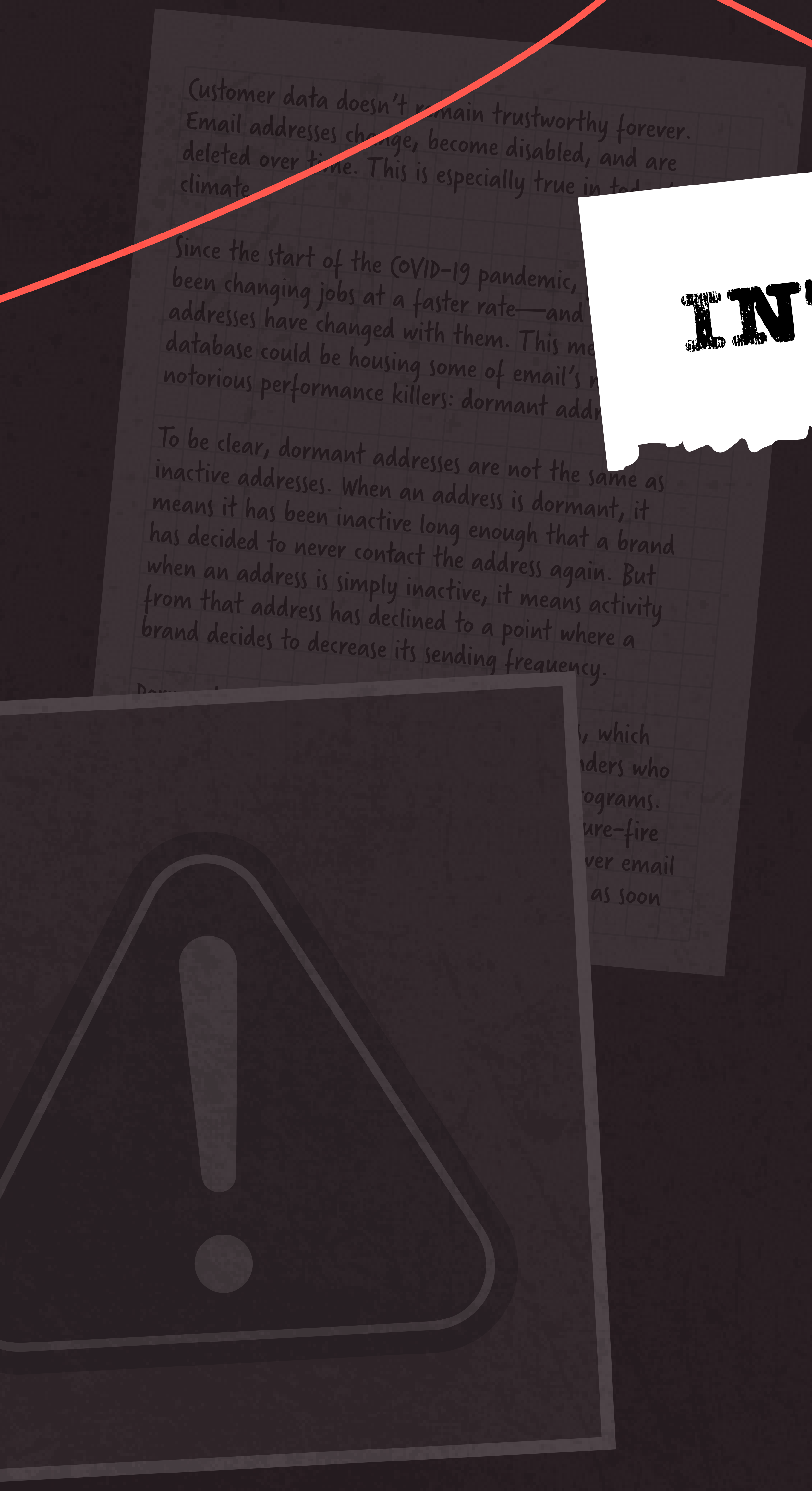


ner data doesn't remain trustworthy forever.
addresses change, become disabled, and are
over time. This is especially true in today's

start of the COVID-19 pandemic, people have
nging jobs at a faster rate—and their email
have changed with them. This means your
could be housing some of email's most
ous performance killers: dormant addresses.

be clear, dormant addresses are not the same as
tive addresses. When an address is dormant, it
ns it has been inactive long enough that a brand
decided to never contact the address again. But
an address is simply inactive, it means activity
that address has declined to a point where a
decides to decrease its sending frequency.

t addresses get recycled as spam traps, which
providers monitor and use to spot senders who
ying lower standards to their email programs.
these addresses in your database is a sure-fire
lower email
as soon



Customer data doesn't remain trustworthy forever. Email addresses change, become disabled, and are deleted over time. This is especially true in to climate

Since the start of the COVID-19 pandemic, been changing jobs at a faster rate—and addresses have changed with them. This me database could be housing some of email's notorious performance killers: dormant addr

To be clear, dormant addresses are not the same as inactive addresses. When an address is dormant, it means it has been inactive long enough that a brand has decided to never contact the address again. But when an address is simply inactive, it means activity from that address has declined to a point where a brand decides to decrease its sending frequency.

, which
nders who
ograms.
ure-fire
ver email
as soon

INTRODUCTION

You crafted compelling copy. Wrote an eye-catching subject line. Implemented personalization techniques. Created a sense of urgency. Tested the campaign design. Heck, you even made sure to send at optimal times based on your recipients' location.

But it wasn't enough.

In the end, your email performance took a turn for the worse. The question is: Why?

We're here to help you solve the mystery.

Here's your first clue: Apart from everything mentioned above, there's one thing that can make or break your email performance—and that's list hygiene.

This process of data validation ensures your email list is comprised of valid and positively engaged subscribers and plays a big role in determining whether your emails make it to the inbox. If your list isn't clean, it can significantly lower your deliverability and have deadly consequences on your email performance.

If our suspicions are correct, we're one step closer to cracking the case.

Now it's time to review our suspect pool. When it comes to list hygiene, there are plenty of suspects that could be killing your email performance. But which one is our culprit?

We're about to find out. Read on to discover the common culprits of poor list hygiene and catch which one is killing your email performance.

Table of contents

This first suspect is often hiding in plain sight.

Single opt-in is a one-step process that requires a person to enter their email address one time in a signup form on your website. Once they enter their address, the new subscriber is immediately added to your list—no confirmation required.

Seems harmless, right?

Not necessarily. The sneaky thing about single opt-in is it doesn't verify that an email is real (or that it even belongs to a human being). This means you could be unknowingly sending mail to fake addresses, which can slowly kill your email performance over time.

Spammers and phishers are notorious for their poor list hygiene, so when mailbox providers notice this type of behavior, they start to become suspicious. Continuously sending to fake addresses is all it takes for a mailbox provider to send your mail straight to the spam folder—or to block you entirely.

Think single opt-in could be the culprit? Protect the quality of your list by implementing a double opt-in process.

Double opt-in requires the subscriber to click on a link sent via email to officially opt in. Since subscribers need to confirm their interest, you can be confident that the people joining your list are eager to sign up. Subscribers who sign up for your email program this way are less likely to report your emails as spam and more likely to engage with your content.

However, not everyone who starts the double opt-in process will end up confirming their interest in your program, which can result in fewer signups. If this concerns you, here are some alternative approaches to consider:

→ Double entry of address
By asking subscribers to enter their address twice, you can verify that the address was entered correctly.

→ CAPTCHA
Implementing this type of challenge-response test can help you prevent bot signups by determining whether a user is human.

Next in our lineup are email bounces. These occur when an email can't be delivered to the inbox. They're incredibly frustrating—and failing to address them could be fatal to your email performance.

Think of bounce notifications as warnings from mailbox providers. The first time you receive a bounce notification, the mailbox provider lets you know something is wrong and gives you a gentle nudge to fix the issue. But if you ignore their warning and continue to send to these addresses, you'll end up on the mailbox provider's bad side—and they may decide to block your email altogether.

Sound familiar? If so, you may have found your culprit.

What you should do next depends on the type of bounce you're receiving.

Hard Bounce

A hard bounce indicates a permanent reason an email cannot be delivered (sender reputation issues, failure to comply with authentication policies, nonexistent domain or email address, etc.). You should remove these addresses from your list automatically to avoid killing your email performance.

Soft Bounce

A soft bounce, on the other hand, indicates a temporary reason an email can't be delivered (mailbox is full, email is too large, email doesn't meet recipient server's anti-spam requirements, etc.). Try sending to these addresses three times before removing them from your list.

It's also important to have a bounce management strategy in place. Senders should review bounce logs on a regular basis to better understand how and why they are being generated.

Although bounce codes are reasonably standardized, they can vary from one MBP to another. An additional challenge is that sometimes permanent conditions generate soft bounce codes, and vice versa. Keeping this in mind can prevent you from unnecessarily suppressing good addresses.

Dormant addresses

Customer data doesn't remain trustworthy forever. Email addresses change, become disabled, and are deleted over time. This is especially true in today's climate.

Since the start of the COVID-19 pandemic, people have been changing jobs at a faster rate—and their email addresses have changed with them. This means your database could be housing some of email's most notorious performance killers: dormant addresses.

To be clear, dormant addresses are not the same as inactive addresses. When an address is dormant, it means it has been inactive long enough that a brand has decided to never contact the address again. But when an address is simply inactive, it means activity from that address has declined to a point where a brand decides to decrease its sending frequency.

Dormant addresses get recycled as spam traps, which mailbox providers monitor and use to spot senders who are applying lower standards to their email programs. Keeping these addresses in your database is a sure-fire way to damage your sender reputation and lower email engagement, so it's important to remove them as soon as possible.

But if you're hesitant to remove inactive addresses from your CRM because you're not sure whether they are still in use, try sunsetting the addresses first. Sunsetting involves removing unengaged subscribers from your email list for a specified length of time. The good news about sunsetting is once you've segmented out the subscribers who fit your criteria, you're not deleting them permanently—you're just setting them aside for the time being.

Just keep in mind that how you view inactivity may differ from how mailbox providers view inactivity. It's no good having a recency threshold of 150 days if Gmail's definition is 30 days. Be sure to research how top mailbox providers define inactivity before determining a recency threshold.

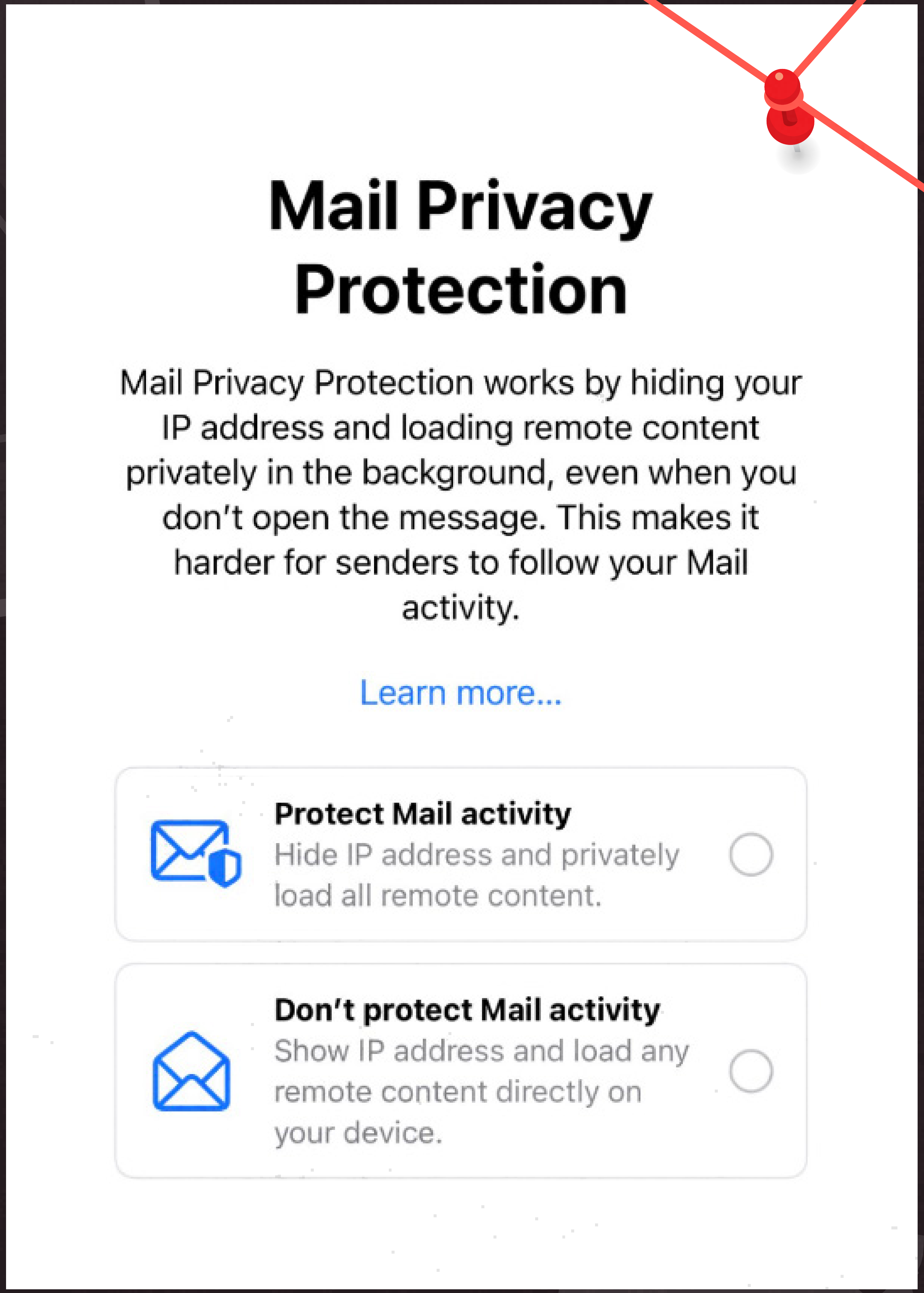
You'll also want to consider the effect Apple's Mail Privacy Protection (MPP) has on subscriber activity. MPP prevents senders from using tracking pixels to measure open rates and device usage and masks recipients' IP addresses to prevent location tracking. It accomplishes this by prefetching and caching email images at the time emails are delivered (as long as the device is connected to the internet).

This means all tracking pixels will fire, regardless of whether the recipient actually opens the message. As a result, open rates skyrocket—but not because more people are truly engaged.

Talk about a smooth criminal!

This provides an unrealistic view of activity, which means senders are more likely to retain addresses believing them to be active while they are actually decaying.

Proactively asking your audience if they're still interested in hearing from you matters even more post-MPP, since your subscribers' engagement levels are now less certain. Try implementing a re-engagement campaign, and after you've made your best attempt to win them back, permanently remove unengaged subscribers from your list.



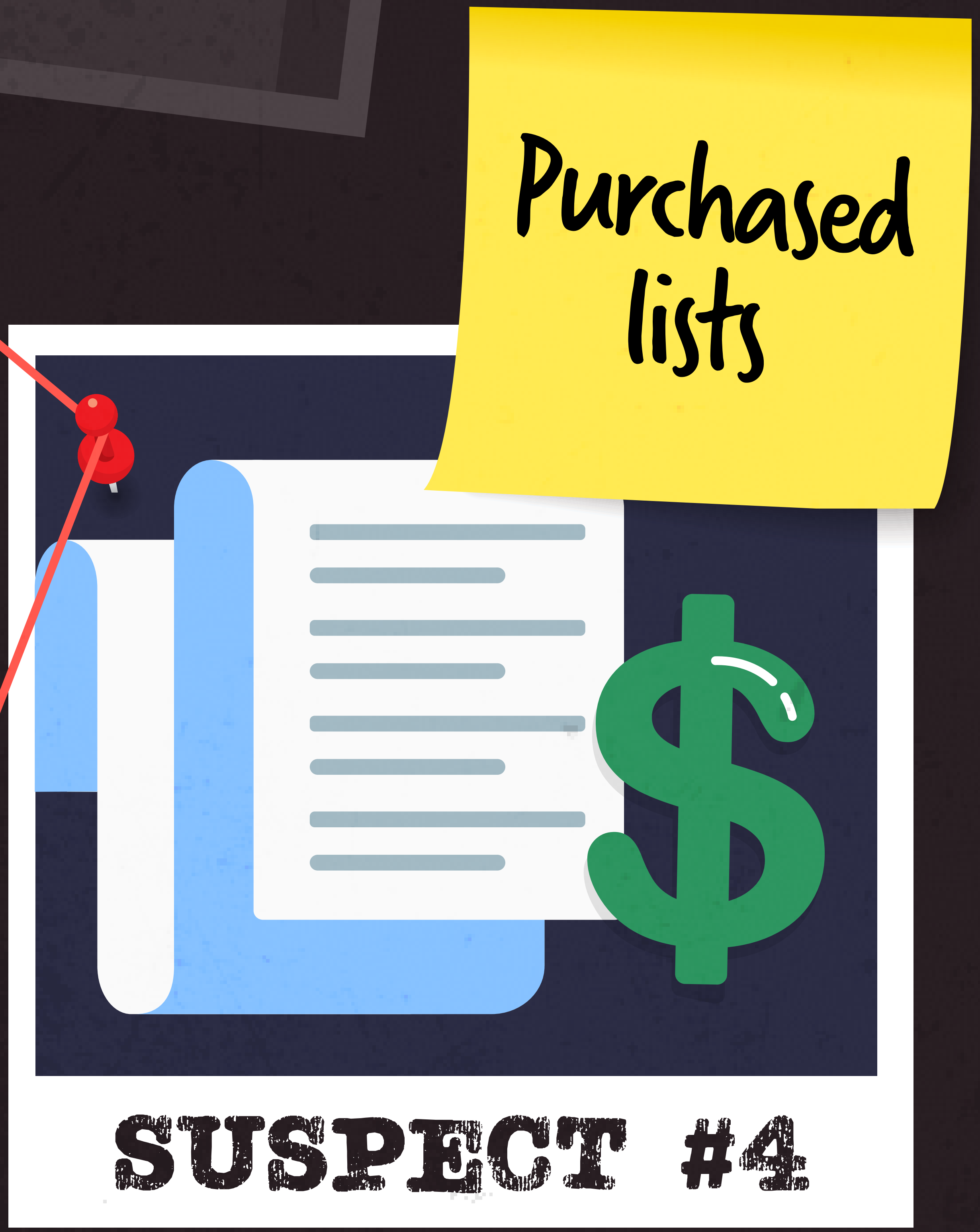
Mail Privacy Protection

Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity.

Learn more...

Protect Mail activity
Hide IP address and privately load all remote content. ○

Don't protect Mail activity
Show IP address and load any remote content directly on your device. ○



Purchasing email lists is a quick and easy way to build your subscriber base—but it's also risky. If you're not careful, taking this gamble can end up costing you way more than the list purchase price (like your sender reputation and deliverability).

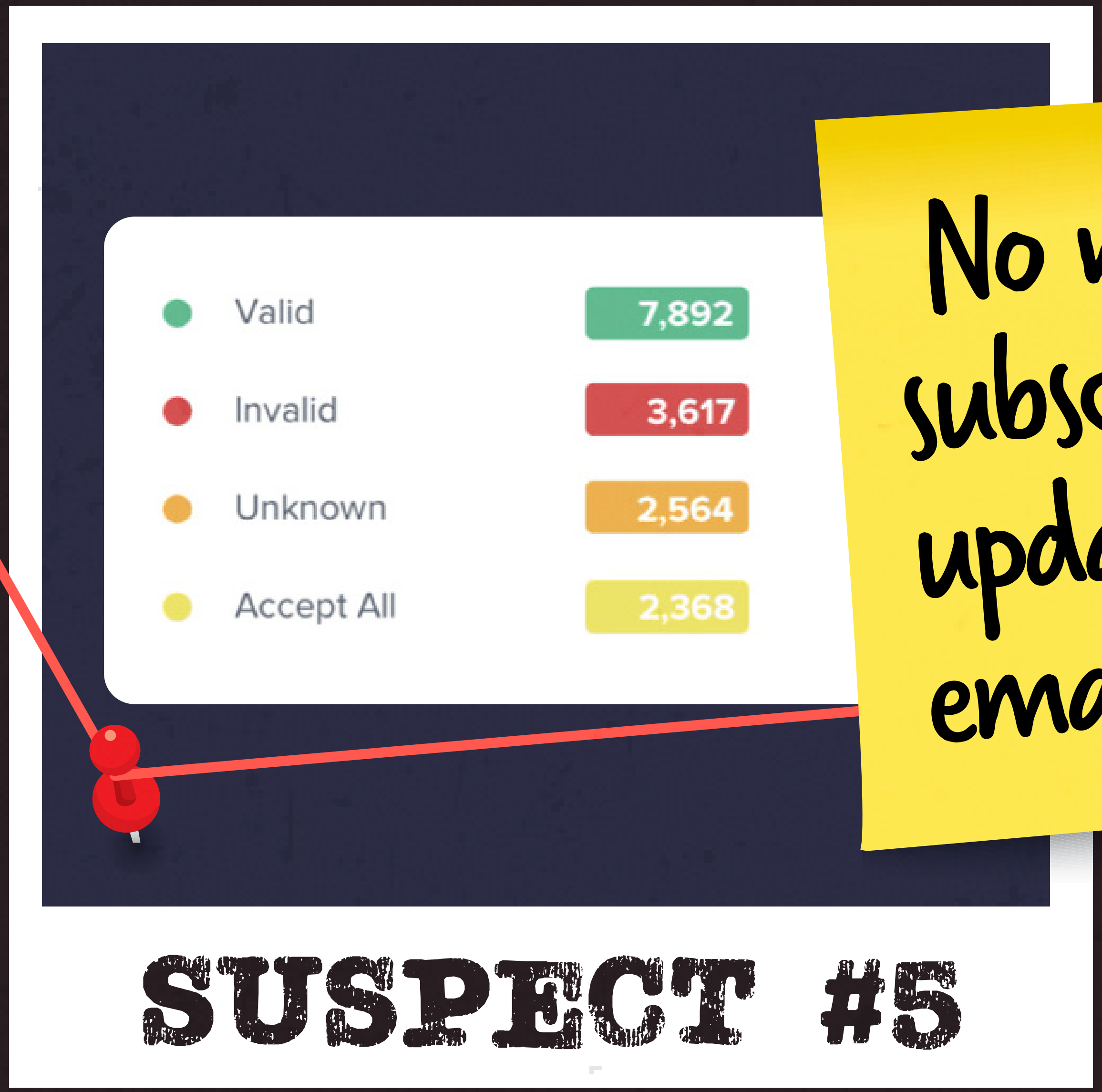
While the people on these lists may be in your target demographic, they don't know or engage with your brand. Buying lists can result in unqualified contacts, increased chances of getting marked as spam, and low engagement—all of which cause poor list hygiene and can kill your email performance.

For these reasons, it's highly advisable to avoid buying lists. But if there comes a time when you decide purchasing lists is what makes the most sense for your business, it's crucial to make sure you're buying lists that are the highest quality possible.

So, how can you do this? Start by doing due diligence to audit how regularly the addresses get used, how the addresses are sourced, and (perhaps most importantly) what consent their owners provided.

Consumers are growing more and more wary of who has access to their personal information and how it's used. In fact, newer global privacy laws make it illegal to mail to people who haven't consented! If you're going to purchase a list, be sure to confirm the addresses on the list were obtained legally and with the owners' consent.

You should also focus on taking the time to build a valuable email list. As more and more mailbox providers narrow in on engagement as a primary factor in spam filtering decisions, building a list of high-quality, engaged subscribers is increasingly important. Start by building a foundation for positive subscriber experiences, exploring different ways to encourage email opt-ins, or promoting your email program when subscribers are offline.



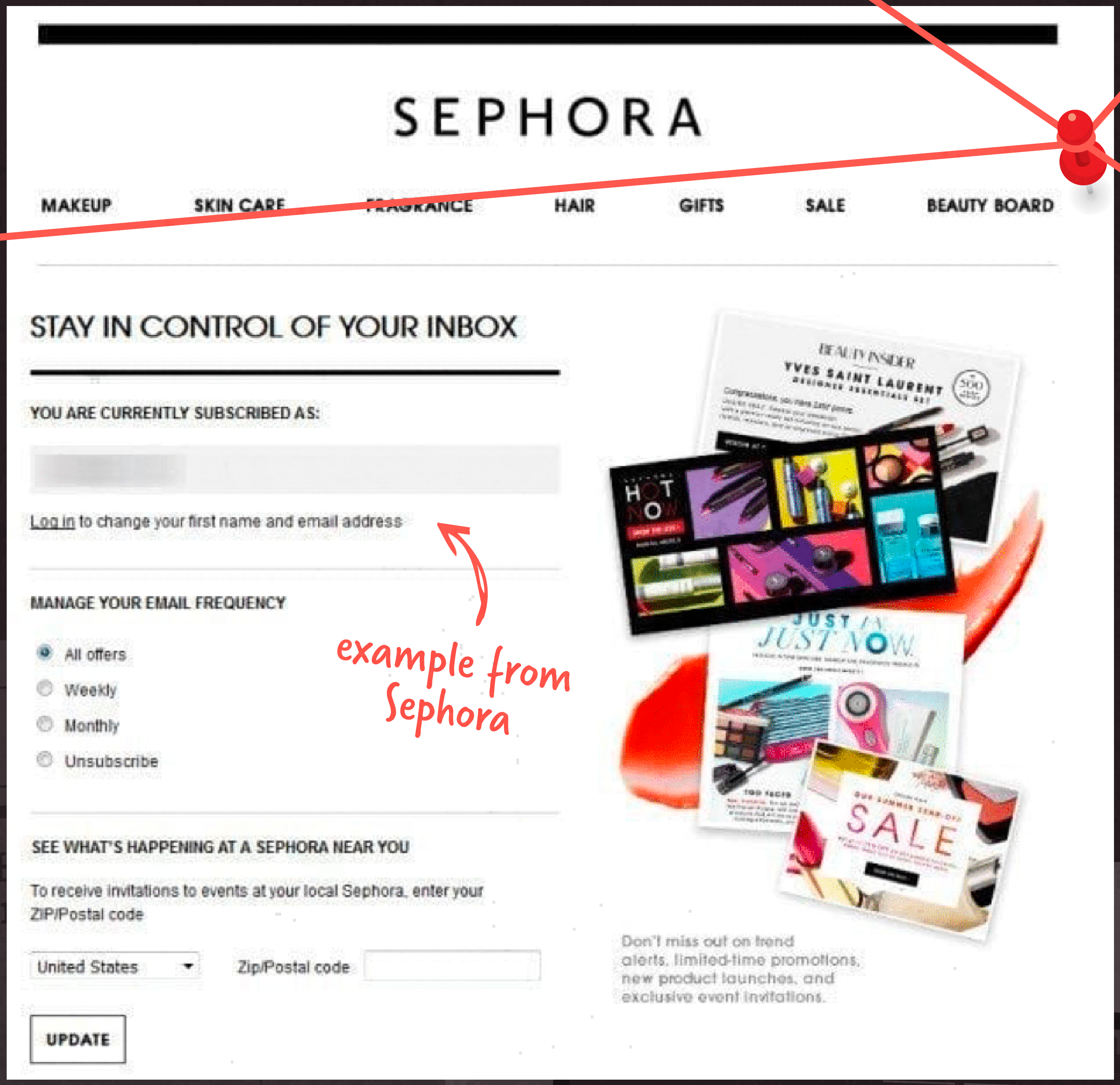
● Valid	7,892
● Invalid	3,617
● Unknown	2,564
● Accept All	2,368

SUSPECT #5

No way for subscribers to update their email address

As we mentioned earlier, your subscribers' information will inevitably change over time. If you continue sending to addresses once they're inactive, you'll garner negative attention from mailbox providers—and a one-way ticket to the spam folder.

The easiest way to avoid landing in email prison? Give subscribers the opportunity to update their email address, either through a preference center, an email change of address (ECOA) service, or in email footers. This allows them to continue engaging with your content and prevents your list data from going stale.



STAY IN CONTROL OF YOUR INBOX

YOU ARE CURRENTLY SUBSCRIBED AS:

[redacted]

Log in to change your first name and email address

MANAGE YOUR EMAIL FREQUENCY

● All offers
○ Weekly
○ Monthly
○ Unsubscribe

SEE WHAT'S HAPPENING AT A SEPHORA NEAR YOU

To receive invitations to events at your local Sephora, enter your ZIP/Postal code

United States ▾ Zip/Postal code

UPDATE

Don't miss out on trend alerts, limited-time promotions, new product launches, and exclusive event invitations.

example from Sephora

NEED TO SEND A POSITIVE SIGNAL

SUSPECT #6

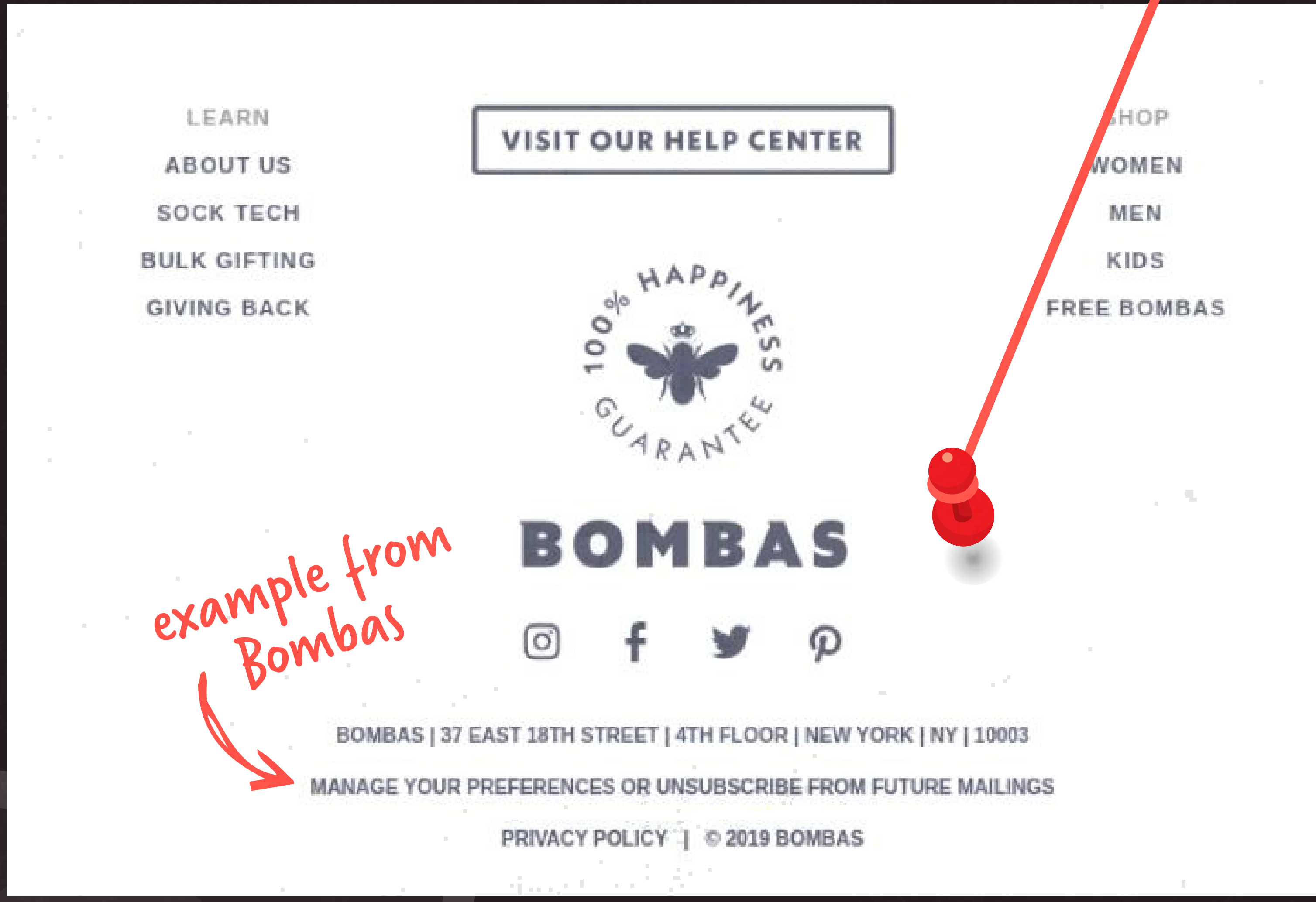
No unsubscribe option

You know what they say: When solving a crime, the perpetrator is usually the person you least expect. That said, if you thought unsubscribes were killing your email performance, think again. It turns out the *opposite* is true.

It may seem backwards, but allowing audience members to unsubscribe from your email program is crucial to maintaining strong email performance. If someone wants to stop receiving your messages and they're not given the option to unsubscribe, they'll fall to the alternative, which is to (dun dun dun...) hit the spam button.

Offer a global unsubscribe option and allow subscribers to unsubscribe from specific email streams via a preference center. But don't stop there—make this option known! Promote your unsubscribe form at the top of your email campaigns, in headers or footers on your website, or even in SMS text messages.

While this will likely result in a higher number of unsubscribes, it will also cause your complaint rate to drop, which is far more important when it comes to deliverability. Spotlighting your unsubscribe option also sends out a positive signal that you're a transparent and trustworthy sender.


LEARN
ABOUT US
SOCK TECH
BULK GIFTING
GIVING BACK

VISIT OUR HELP CENTER

100% HAPPINESS GUARANTEE

BOMBAS

SHOP
WOMEN
MEN
KIDS
FREE BOMBAS

BOMBAS | 37 EAST 18TH STREET | 4TH FLOOR | NEW YORK | NY | 10003
MANAGE YOUR PREFERENCES OR UNSUBSCRIBE FROM FUTURE MAILINGS
PRIVACY POLICY | © 2019 BOMBAS

example from Bombas

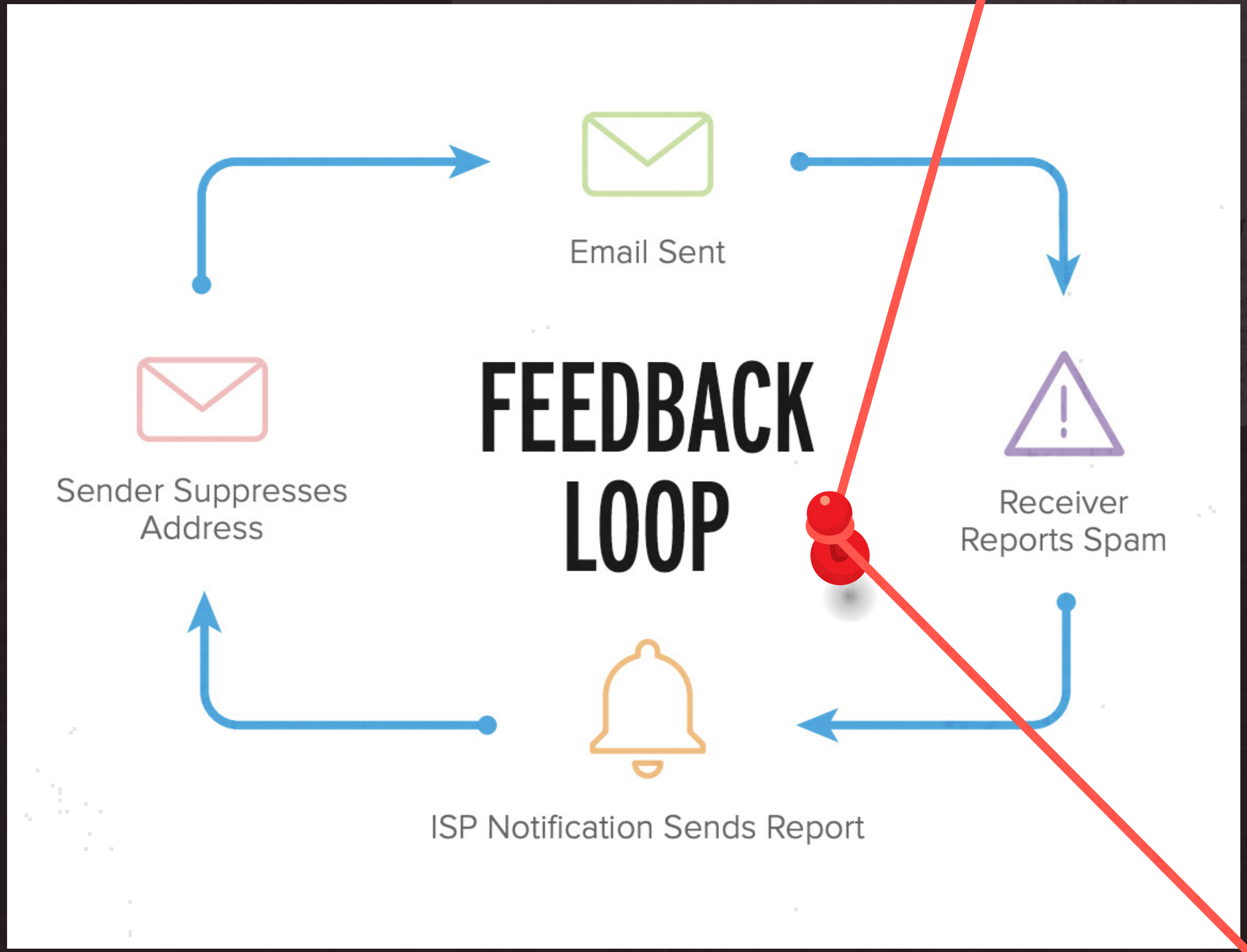
Lack of feedback

SUSPECT #7

Imagine you're getting ready to turn in for the night when you hear loud music coming from your neighbor's house. Frustrated, you pick up the phone and call the police to file a noise complaint. Your other neighbors do the same. The police visit your neighbor's house later that evening and tell them to quiet down before they're asked to pay a fine.

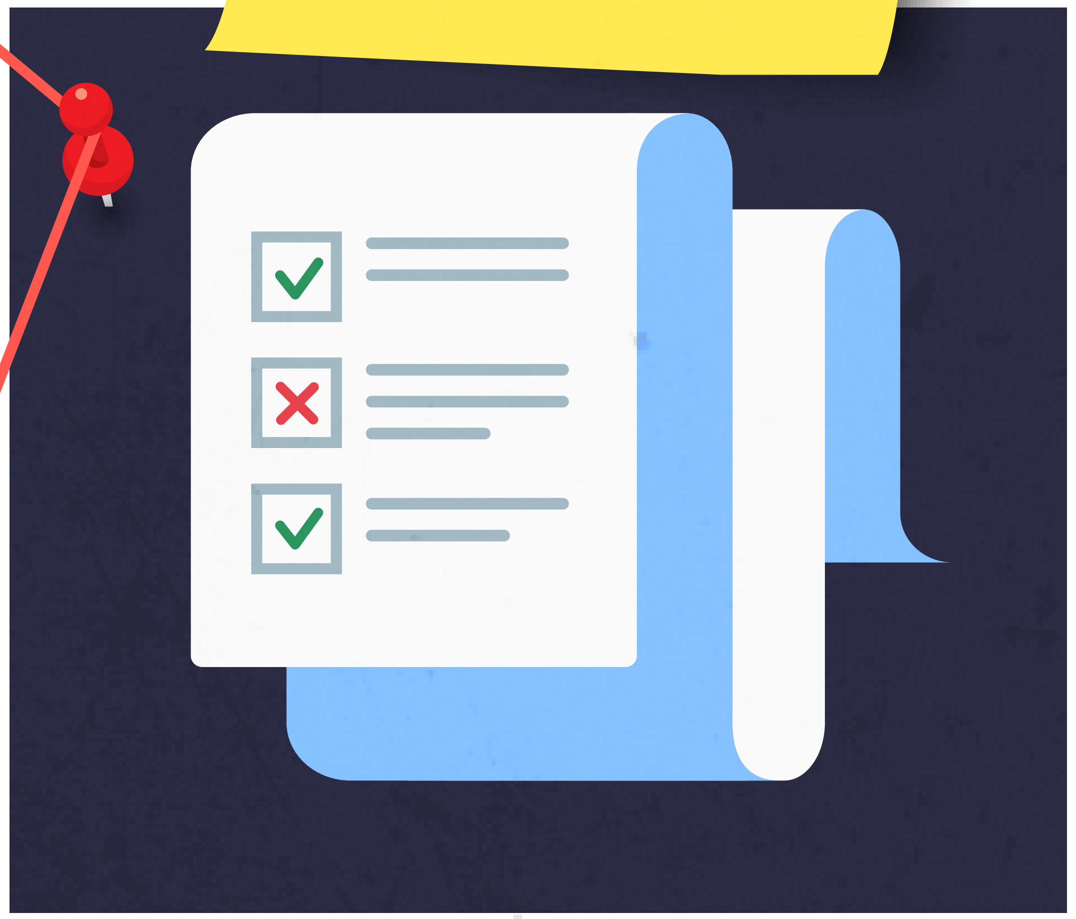
In this case, the police were able to warn your neighbor about the complaints before they got into serious trouble. In the email world, a feedback loop can do the same for you and your email program.

If you're not currently signed up for a feedback loop, there's a very good chance that's what's killing your email performance. A feedback loop enables an internet service provider (ISP) to inform you about spam complaints submitted by recipients of your messages. Being signed up for a feedback loop means you can remove these email addresses from your list, ensure they don't continue receiving unwanted messages from you, and avoid spam complaints.



For example, Validity has partnered with over two dozen mailbox providers to provide a universal feedback loop management service for organizations sending large amounts of mail. The feedback loop will forward any mail reported as spam originating from the associated IP addresses and/or domains back to the listed email address. We highly recommend the use of a dedicated email address for this purpose.

Manual list validation



SUSPECT #8

Perhaps the most likely suspect in our lineup is manual list validation.

As you've seen throughout the previous sections, there are many ways for invalid addresses to make their way onto your email list. Since manual list validation is a tedious process that requires exceptional attention to detail, the probability of human error and oversight is high. This means some of the invalid addresses on your list will likely go undetected, which can poison your email performance in the long run.

But that's not all. Manual list validation can also waste valuable time that would otherwise be spent crafting killer subject lines, brainstorming juicy content, or training to become the next American Ninja Warrior (if you're into that sort of thing).

Get those hours back and prevent oversight by implementing a real-time list validation tool. List validation enables you to quickly identify and remove addresses that no longer exist, as well as invalid, fake, typo, and risky email addresses (e.g., role accounts and disposable addresses) from your lists before you send your campaign.

In addition to list validation, you can set up rules to confirm address structure or lookup tables with commonly malformed domains. It's also a good idea to periodically review the full email database for domains that report zero open or click activity. These domains are either invalid or blocking the sender and should be suppressed.

Lastly, it's important to double check for any bot signups that may have made it onto your list. Check for addresses that click on all links near-simultaneously or include a "hidden" link in your email that a human recipient would never use.

Now for our final suspect: spam traps.

Spam traps are some of the deadliest email traps of all. They're set by anti-spam organizations, ISPs, and corporations to highlight bad email practices. If you're not proactively taking steps to keep your list clean, you may end up with spam traps on your contact list.

If you're sending mail to spam traps and trap owners catch you red-handed, this will result in some form of punitive action. For example, you may experience more filtering, or your IP address or even your domain could be blocklisted. In turn, this affects your sending reputation, deliverability, and (you guessed it!) your email performance.

There are three main types of spam traps to be on the lookout for:

→ Recycled spam traps

Recycled spam traps are addresses that were legitimate addresses at one point in time but have been repurposed to catch abusive mail. These can end up on your list if you're not staying on top of recency management.

→ Typo spam traps

Typo spam traps are addresses that contain a typo, usually in the domain (e.g., bobsmith@gnail.com instead of gmail.com). Typo traps can be found mostly on major email domains like Yahoo!, Gmail, AOL, and Outlook.com. If you don't have any list validation measures in place, your list is highly susceptible to typo traps.

→ Pristine spam traps

Pristine spam traps, also referred to as honeypots, are email addresses created with the sole purpose of capturing spammers. These addresses were never legitimate destinations, do not subscribe to email programs, and do not make purchases. You're likely to end up with some of these on your list if you haven't taken the proper measures to acquire addresses legally and with the owners' consent.

Since they need to be anonymous, spam traps are not easy to identify. Therefore, following list hygiene best practices (like the ones mentioned in the previous eight sections of this guide) is your best defense against these sneaky offenders.

If you're taking steps to keep your list clean, you should have very little to worry about! However, it's still best practice to monitor for spam traps just in case.

TURN YOUR LIST INTO A CLEAN, MEAN, PERFORMANCE-BOOSTING MACHINE

get a free demo

Great work, detective! We've made it through our list of suspects. Now grab some coffee, sit back, and take some time to look over the evidence.

Think you've identified the culprit?

Good. But we should warn you: the suspects on this list tend to be repeat offenders. You may have caught the culprit and saved your email performance this time around. But if long-term measures aren't taken to improve your list hygiene, your email program may not survive the next time one of these culprits decides to attack.

In today's unpredictable climate, you can't afford not to invest in the quality of your list. Ensure the cleanliness of your list by implementing a contact verification solution like BriteVerify, from Validity. BriteVerify provides secure, scalable validation so you can build and maintain an actionable database, reach more people, and communicate more effectively.

To learn more about how BriteVerify can help you catch the culprits of poor email performance, schedule a free demo today with one of our experts.

Businesses run better and grow faster with trustworthy data. Tens of thousands of organizations rely on Validity solutions – including Everest, DemandTools, BriteVerify, GridBuddy Connect, and MailCharts – to target, contact, engage, and retain customers effectively. Marketing, sales, and customer success teams worldwide trust Validity solutions to help them create smarter campaigns, generate leads, drive response, and increase revenue.

For more information visit validity.com and connect with us on LinkedIn and Twitter.

validity.com
sales@validity.com