I’ve gotta BIMI

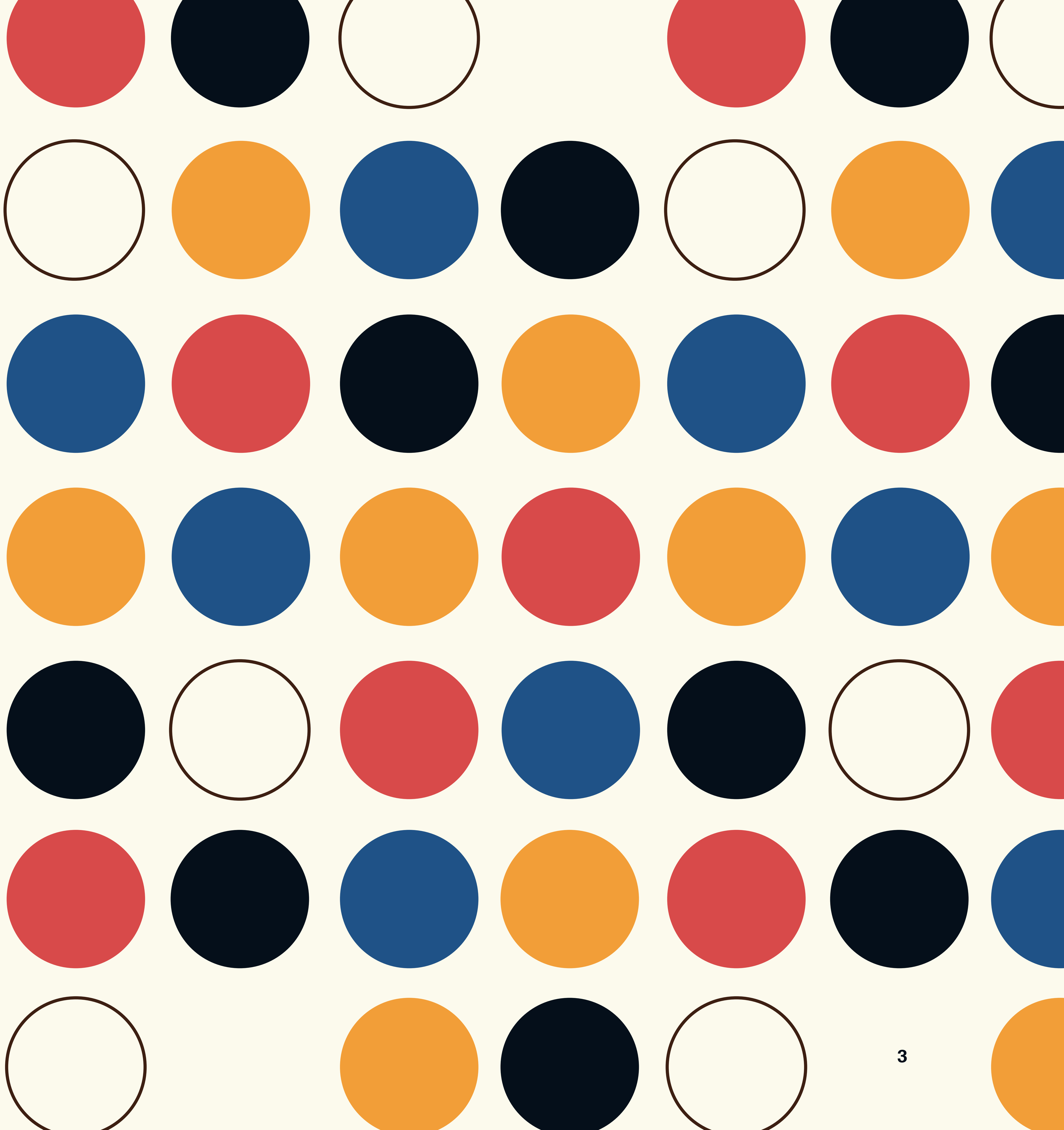
Table of Contents

Introduction

Yes, we are here with another acronym for your email repertoire. Brand Indicators for Message Identification, or "BIMI" as the kids say, is one of the newest technologies for email. Any marketer trying to capture the spotlight in a chaotic inbox needs to become familiar with BIMI sooner rather than later.

In this eBook, we'll walk you through the technology, why it's important, and what you need to do to adopt BIMI.

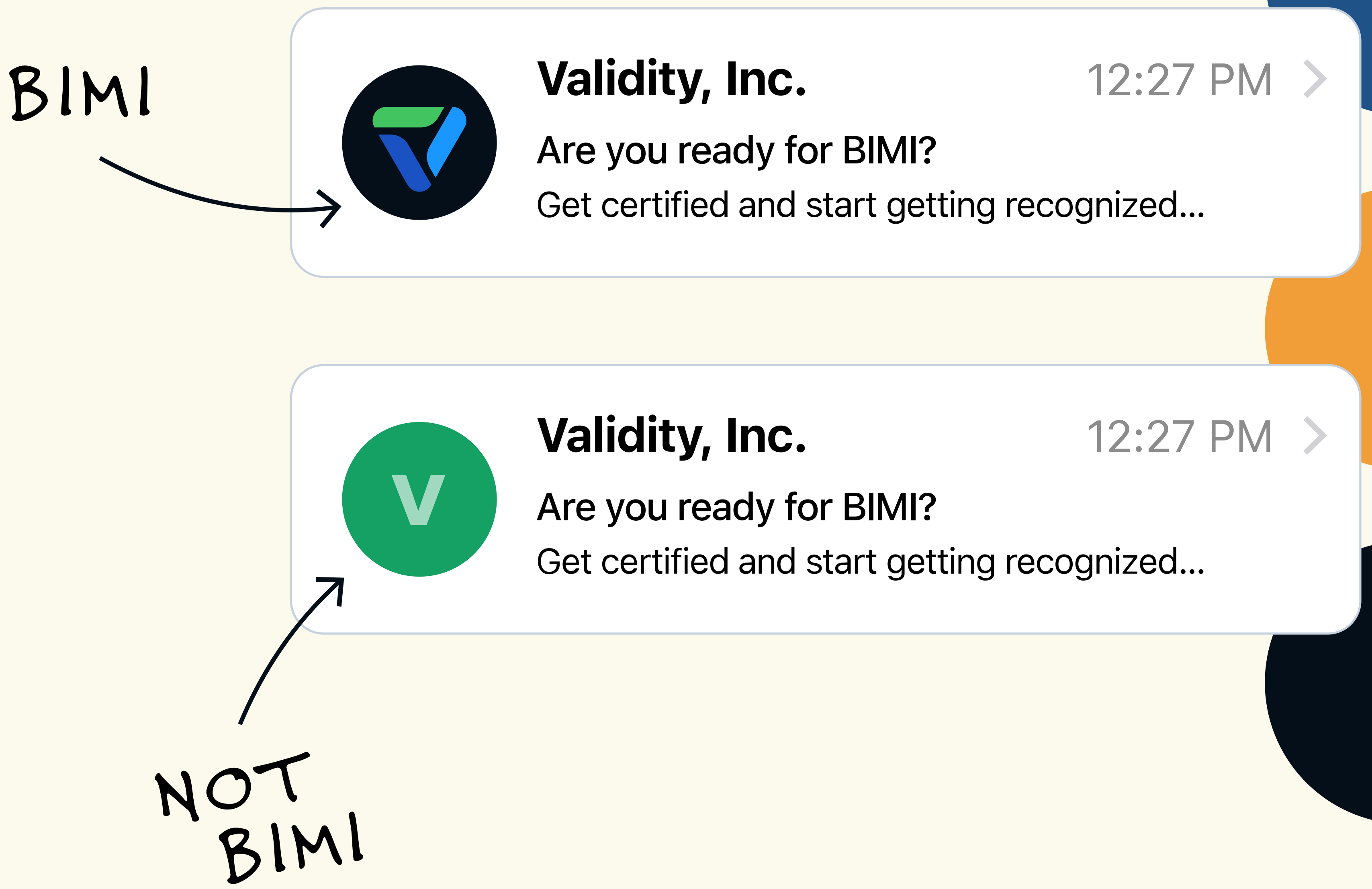
BIMI up, Scotty, we're ready to fly.



Tell "MI" More About BIMI

At the simplest level, Brand Indicators for Message Identification is a little photo or "indicator" next to the name of the sender associated with an email sitting in the inbox. Imagine getting an email from Target about a sale, and to the left of the email is a small picture of the Target logo.

Right now, specific implementations will vary by mailbox provider (MBP), but at the most basic level, you need a valid BIMI record, 100% DMARC enforcement (more on that later), and a good sender reputation. BIMI is not supported by every MBP, but it is supported by email giant Gmail, plus others like Yahoo, AOL, and Verizon inboxes. This means if you're emailing Gmail users and you have BIMI in place, the recipient will see your logo associated with all the email you send to the inbox.



Validity, Inc. 12:27 PM

Are you ready for BIMI?

Get certified and start getting recognized...

Validity, Inc. 12:27 PM

Are you ready for BIMI?

Get certified and start getting recognized...

Why is BIMI for “MI”?

Let’s go back to our earlier Target example. You get a Target email, and before you even see the word “Target” or “An incredible sale in which you intend to buy one thing and instead buy 100,” you see the Target logo. Boom. Bullseye. You’re putty in their hands.

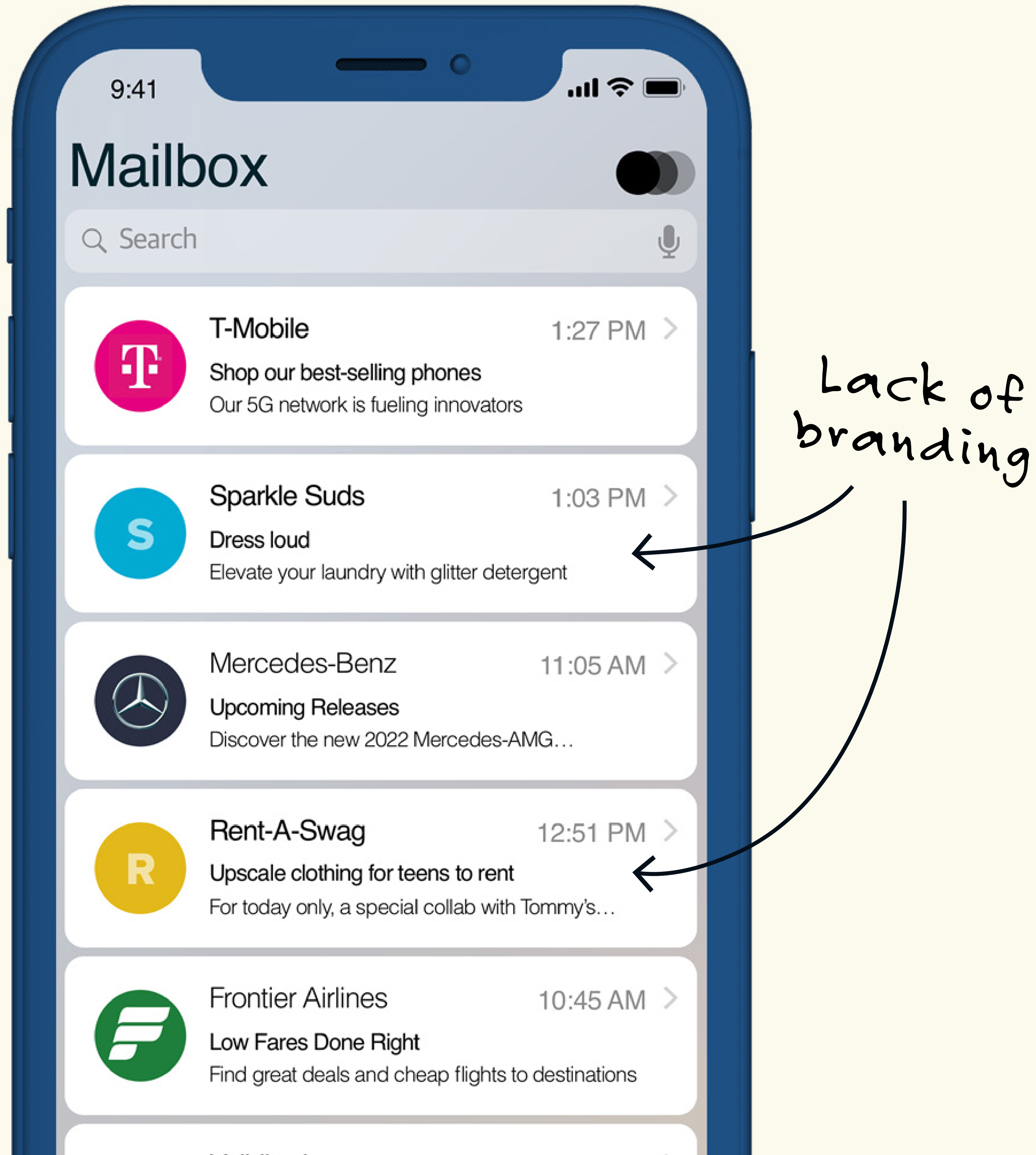
You immediately connect the email to the brand, without even needing to read the subject line or sender. The logo tells you all you need to know – the email is from Target, and we all love Target. Can’t deny it.

BUT. Having said that, bigger brands like Starbucks can get lost in the inbox without a logo, especially if the red-headed stepchild Dunkin Donuts does have a BIMI graphic. This is another huge benefit of BIMI.

The inbox is stuffed. Double stuf’d. Emails without BIMI logos are relatively plain – no visual interest, no fabulous disco ball of colors drawing you in. With a bright logo to capture the eye, any email with a BIMI logo is more likely to break through the repetition of text on text.

Today, this can make all the difference.

Finally, the last reason is to protect your own brand. Completing the email authentication requirement is the most important aspect of BIMI, so it deserves more than a paragraph. It gets its own chapter. Here it is.



9:41

Mailbox

Search

T-Mobile 1:27 PM
Shop our best-selling phones
Our 5G network is fueling innovators

Sparkle Suds 1:03 PM
Dress loud
Elevate your laundry with glitter detergent

Mercedes-Benz 11:05 AM
Upcoming Releases
Discover the new 2022 Mercedes-AMG…

Rent-A-Swag 12:51 PM
Upscale clothing for teens to rent
For today only, a special collab with Tommy’s…

Frontier Airlines 10:45 AM
Low Fares Done Right
Find great deals and cheap flights to destinations

Lack of branding

How do I BIMI?

Now it gets technical – but you're ready, since you know why you need BIMI and how you qualify. It boils down to two words: **email authentication**.

There are so many email-related scams, like phishing, in which someone imitates a legitimate sender (usually shockingly well) to try to extract personal information from recipients. Without putting protections in place, your brand is open to hijacking, resulting in damage to your brand, your reputation, and in worst case scenarios, the security or finances of your customers.

While your subscribers won't necessarily see BIMI and think, "Wow, they're very serious about email security, bless their hearts," the fact remains you need to have your security on lock to use it.

You'll need to get familiar with three major email authentication concepts to unlock BIMI.

SPF

Sender Policy Framework

While this kind of SPF doesn't protect you from the fiery rays of the sun, email SPF protects you from fiery MBPs refusing your mail because they lack the info needed to confirm it's legit. Within the TXT record, there's an indicator that shows whether the IP is approved to deliver mail on behalf of a particular domain. It should validate against the sender header, which is typically your own domain, or the domain of your email service provider (ESP). There are a whole bunch of ways to configure your SPF, but at the end of the day, it's a simple step in convincing MBPs your mail can be delivered safely.

DKIM

DomainKeys Identified Mail

Now you're leveling up the complexity. Unlike a plain TXT record like SPF, DKIM requires the use of an encryption program to generate tokens, keys, and other knickknacks. For our purpose today, you don't need to know enough about DKIM to become the Encrypt Keeper, but know this: The encryption program will use keys and tokens to verify nothing's gone astray during the mail's journey. For instance, the sender information hasn't changed during transmission, or anything within the body of the email got tinkered with on its way.

DMARC

Domain-based Message Authentication, Reporting & Conformance

Lots of people will tell you DMARC is unnecessary, and that if you have SPF and DKIM configured, you're protected on par with the majority of other senders. This is mostly false, but partly true. Sure, without a DMARC record, you're pretty much on level-footing with the majority of senders across industries. However, that's not a great thing. DMARC is an added layer of email protection, and all senders can benefit from the additional layers of monitoring, reporting, and action it provides.

As a sender, you publish a DMARC policy to determine what action the MBP should take when an email fails authentication (both SPF and DKIM). DMARC is applied over time with graduating policies, each directing MBPs to take more severe action as time moves on.

First, a p=none policy advises the receiver to simply do nothing and deliver the mail. Once you have p=none in place, you'll get DMARC reports to give you a grasp of the unauthenticated mail flowing from your IP or domain. Then, move on to p=quarantine, telling the receiver to put that bad boy directly into the spam folder. The final level of protection is p=reject, which basically tells it like it is: Unauthenticated mail should not be delivered, period.

p=none ✗

p=quarantine ✓

p=reject ✓

You must enforce a DMARC policy of p=quarantine or p=reject at 100% to use BIMI.

Until our email-loving society can reliably put bad emails in the trash because they smell like PHISH, using all these protections better ensure you're keeping them out of harm's way. Don't forget, a phishing scam can burn your brand reputation. Email authentication is the best defense you have.

Once you have this in place, you're not totally copacetic yet. You'll need to make a Scalable Vector Graphic (SVG) Tiny PS version of your logo. It's going to be teensy weensy and look very cute in the inbox – highly recommend. Once you've got that, create a BIMI record for your domain in DNS, and bam! You're in like flint.

Help.

Yes. We're happy to help. In fact, it's why Everest exists.

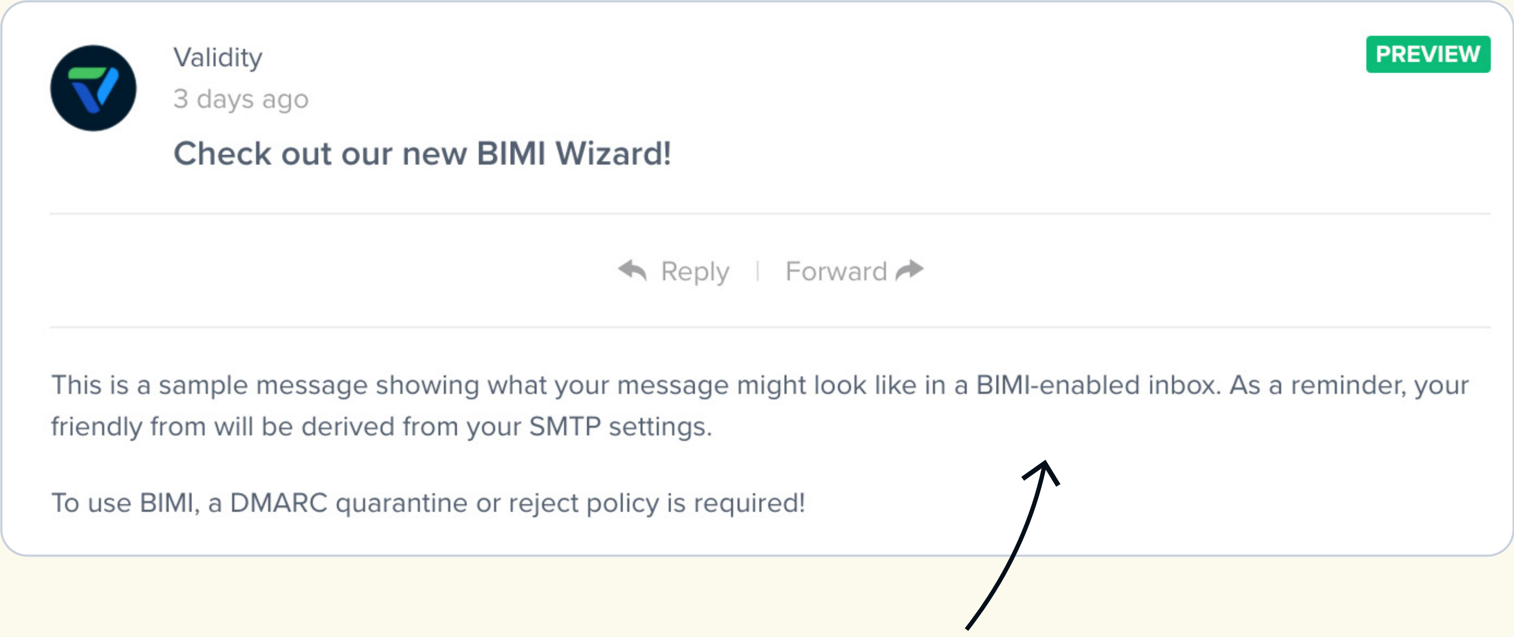
It's important to follow sound guidance when trying to do something as rigorous as BIMI-level email authentication. Not only can Everest confirm your SPF and DKIM policies are aligning and your mail is traveling smoothly to the inbox, but it also provides the tools you need to monitor the performance of your authentication policies.

Everest also has a BIMI tool, which makes implementing BIMI much less complicated than qualifying for the technology in the first place. Everest users can host the BIMI image and preview the way the message appears in BIMI-enabled inboxes. It'll even pop out the BIMI DNS code for you to input at your DNS provider.

These are all pretty straightforward steps in the process, but having a good sender reputation is part science, part witchcraft and wizardry. Your email sender reputation is unique and made up of a bunch of tiny moving parts. Everest is designed to help you monitor all the parts while providing insights and guidance to keep your sender reputation 100, which is exactly what Everest was made to do.

See? We're here for you.

We've also got experts to support your BIMI journey, whether you find email authentication challenging or you're struggling to improve your reputation to "baller" level. Once you've enabled BIMI, Everest will give you the important stuff: the proof BIMI is worth the effort. First, you should run design tests on BIMI-enabled MBPs to ensure the logo is showing up as intended. Once you're sure it's working, Everest users can keep a keen eye on email engagement. Notice changes in open rates between pre- and post-BIMI implementation? Experiencing an exhilarating bump in clicks or conversions after trying BIMI? Everest helps you connect the dots.



Validity
3 days ago
Check out our new BIMI Wizard!

This is a sample message showing what your message might look like in a BIMI-enabled inbox. As a reminder, your friendly from will be derived from your SMTP settings.

To use BIMI, a DMARC quarantine or reject policy is required!

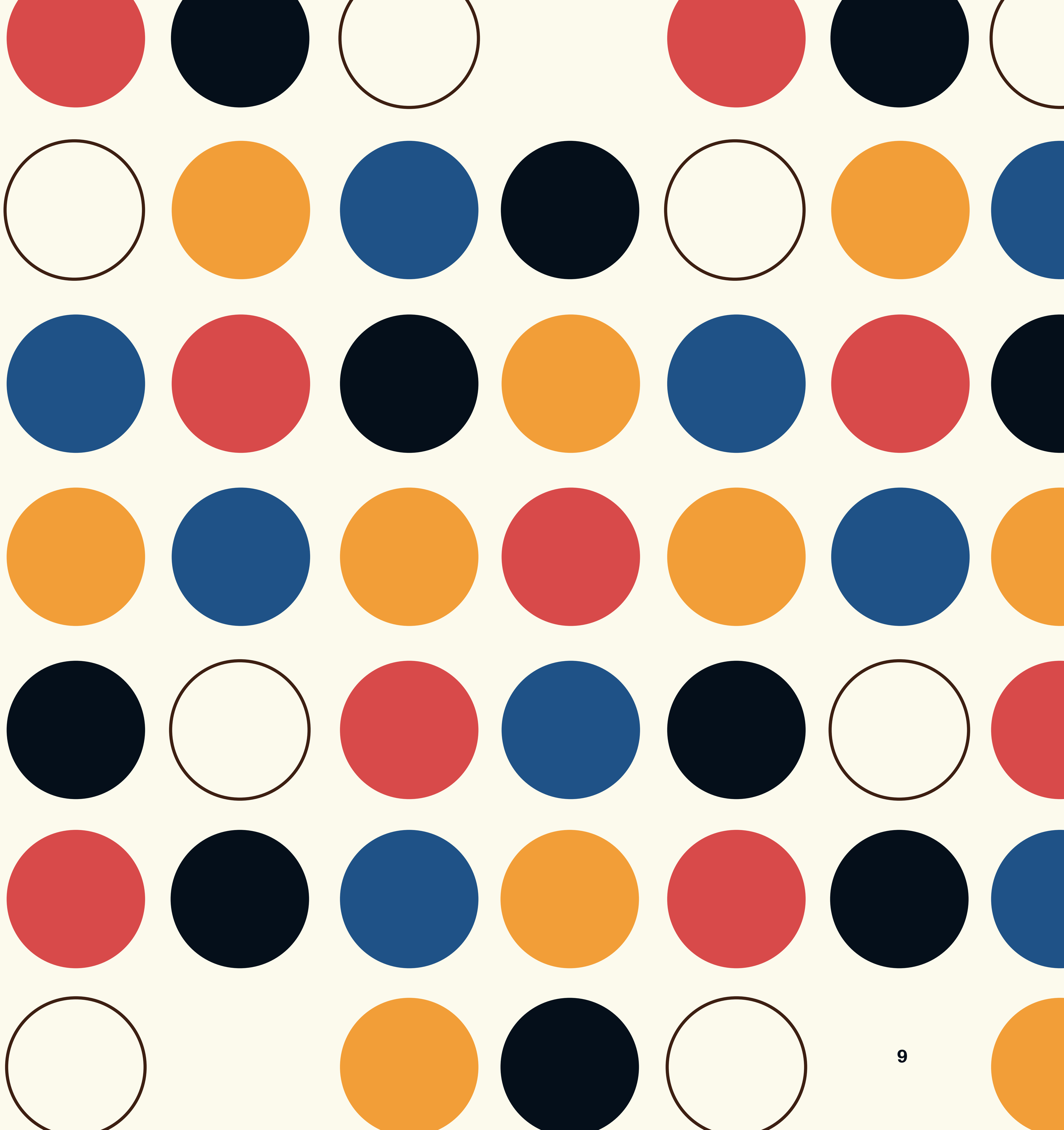
Preview BIMI in Everest!

Conclusion

That's all, friend. You're educated in the art of BIMI. Go forth and strengthen your position in the inbox with another brand impression. If you want to understand DMARC and how to get there in more depth, we already have this **eBook** ready for you.

Sleep easy knowing you ran the email authentication gauntlet to get you there. And if you tend to wake up in the middle of the night panicking over BIMI, you can get even more, yes MORE, information about the technology, tools to help you, and extra goodies from the **BIMI Working Group**.

See you next time!



validity

Businesses run better and grow faster with trustworthy data. Tens of thousands of organizations rely on Validity solutions – including Everest, DemandTools, BriteVerify, Trust Assessments, and GridBuddy Cloud – 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