PATHWIRE

EBOOK

The path to BIMI implementation

What email marketers can expect

Summary

Introduction

The email inbox is irreplaceable. Things change fast on the internet and email has been around for 50 years. Yet it remains an essential part of the digital experience. Email is a communication tool, a personal identifier, and a way to connect with trusted brands.

Unfortunately, the inbox can also be a scary and even dangerous place for your subscribers.

Criminals use email to conduct all sorts of shady activities. Chief among them is a type of phishing known as email spoofing. That's when scammers impersonate your brand with fake emails and web pages. They use those tricks to commit identity theft and get people to offer up sensitive information or download malware.

Cybercriminals understand the power of the inbox, and they abuse it. While you've received permission, built trust, and earned your subscribers' attention, others take advantage of that hard work and deceive people.

Email spoofing must be stopped. It drives mailbox providers crazy, causes serious problems for consumers, and ends up damaging your brand's reputation.

Thankfully, there are ways to prevent phishing attacks that impersonate your brand. The problem is, too few brands are implementing email authentication protocols effectively.

Could a new email standard, known as BIMI, be the nudge brands need?

In this guide, we'll dive into the details of Brand Indicators for Message Identification (BIMI). You'll discover the most important benefits, what's required to get BIMI working, and what the future holds for this technology.

Along the way, you'll hear from the people behind BIMI, email marketers with firsthand experience, and Pathwire's deliverability experts.

PART 1

Email authentication 101

Before we start exploring BIMI, you'll need a baseline understanding of the other email authentication protocols. Here's a quick refresher...

Why do we need email authentication?

Short answer?

To prevent email spoofing and phishing.

Long answer?

Simple Mail Transfer Protocol (SMTP) lacks any way to authenticate whether emails come from who they say they're from before reaching the inbox. Email is built on SMTP. So, people created additional protocols to help receiving mail servers and sending mail servers communicate with each other about the legitimacy of an email.

Three existing protocols are used for email authentication: SPF, DKIM, and DMARC.

Sender Policy Framework (SPF)

This DNS record is a list of **IP addresses** that are approved for sending mail on behalf of your domain. Mailbox providers check SPF records to see if certain hostnames and IP addresses (such as your ESP's) are on the list before delivering a message. Without SPF, you could experience email deliverability issues.

Learn more about SPF

DomainKeys Identified Mail (DKIM)

This method uses an encrypted key called a digital signature, which is attached to outgoing emails. Mailbox providers refer to a public key in the DKIM record on the sender's DNS and look for a match to help verify an email's authenticity.

Learn more about DKIM signatures

Domain-based Message Authentication, Reporting and Conformance (DMARC)

A DMARC policy tells mailbox providers to look for SPF, DKIM, or both protocols. Then, it provides information on **how to filter emails that fail authentication**.

- A policy of none doesn't specify any action.
- A policy set to quarantine means authentication failures should be filtered into spam or blocked.
- A policy set to reject means unauthenticated emails should be blocked and reported to the domain owner. There are also DMARC reports, which provide information about who's sending emails claiming to be from your domain.

Learn more about DMARC policies

> ***If you take away anything from this guide it should be this:***
> *A successful BIMI implementation requires a DMARC policy set to either quarantine or reject.*

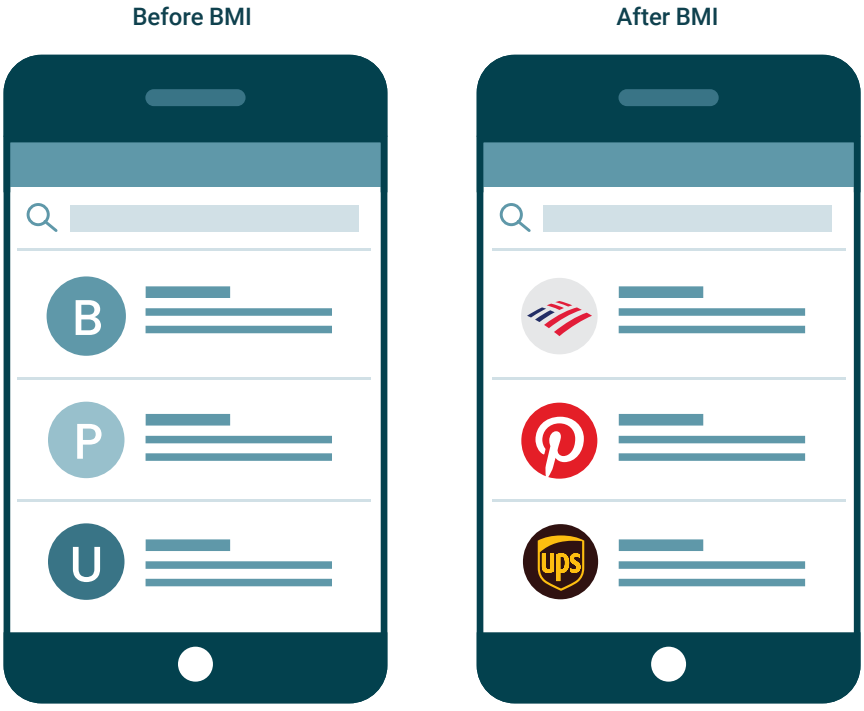
PART 2

BIMI: What it is and why it helps

BIMI is a TXT record published on your sending domain's DNS that mailbox providers reference when determining the authenticity of an email.

BIMI is the final factor in a set of protocols designed to stop email forgery. It's a finishing touch, like the cherry on top of an email authentication sundae.

When BIMI is implemented correctly, a verified logo can appear next to emails in the inbox and at the message level. Unlike SPF, DKIM, and DMARC, BIMI displays verified email authentication in a way your subscribers will see for themselves.



BIMI offers a few potential benefits:

1. Branding in the inbox

BIMI helps build a more immersive email experience for recipients while giving email marketers more control and consistency. It is a standardized way of getting the correct logo to display in various email clients. Ultimately, this increases brand impressions and supports brand recall.

2. Improved email security

On its own, BIMI will not necessarily make your brand's emails more secure. However, to get a BIMI logo to display, you'll need other email authentication protocols in place. Specifically, **you must have a strong DMARC policy** while using SPF, DKIM, or both. In many ways, BIMI logos are meant to motivate brands to pursue stronger email authentication.

3. Increased email engagement

Early user experience studies (UX) suggest the presence of logos in email produces positive results. **Marcel Becker, Sr. Director of Product Management at Verizon Media Group**, says user testing found an experience that included logos beat those that didn't. This could also have a downstream, indirect effect on email deliverability, even though BIMI has no direct effect on inbox placement.

"The more engagement you have with your emails the better your reputation could be. And that might have a positive impact on deliverability."

Marcel Becker, Verizon Media Group

Plus, as consumers begin to look for BIMI logos as a sign of authenticity, they'll feel confident that legitimate emails are safe to open and links are safe to click. It's a visual cue that messages are coming from your brand and not a scammer.

A more recent study from Red Sift and Entrust gives us some hard numbers on how consumers respond to BIMI. A survey of more than 1,000 adults in the U.S. and U.K. suggests that BIMI brand logos:

- Increased **open rates** by 21%.
- Boosted **brand recall** by 18%.
- Improved the **likelihood of purchase** by 34%.
- Increased confidence in the **legitimacy of an email** by 90%.

Discover more insights on how BIMI may impact the email experience and your overall metrics. Get the white paper Consumer Interaction with Visual Brands in Email to explore the full study.

PART 3

The evolution of BIMI

BIMI is an innovation from the Authindicators Working Group, which is now better known as the BIMI Group. It was formed in 2015 and set out to solve a couple of notable problems in the email industry. **Alex Rubin, Pathwire's Sr. Director of Strategic Partnerships**, was part of the group in its early days.

"The impetus for BIMI was two-fold. Primarily, mailbox providers want to promote authentication and best practices around DMARC. They also struggled a bit with sourcing brand logos."

Alex Rubin, Pathwire

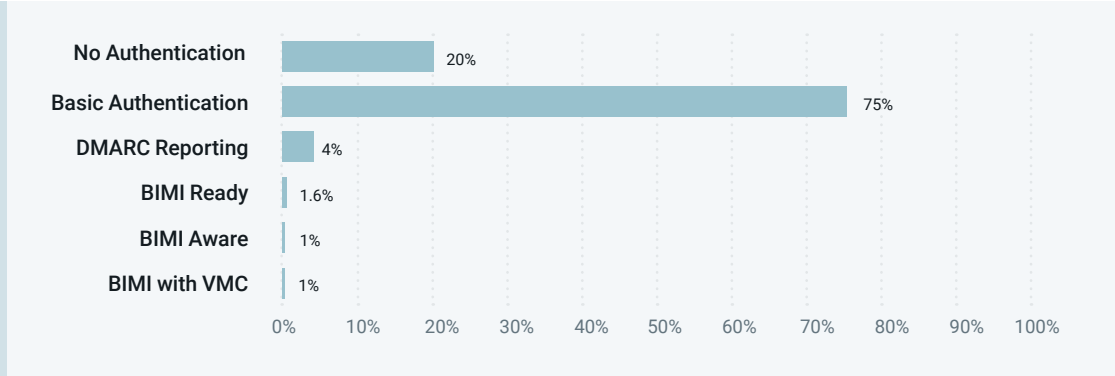
So, how does BIMI help solve these two problems?

Problem 1: Promoting email authentication

While DMARC entered the email authentication scene around 2015, many senders have been slow to adopt it. The website BIMI Radar examines more than 51-million domains and tracks how those domains approach email authentication.

As of late July 2021:

- 75% have basic authentication in place.
- 4% are getting DMARC reports without strong enforcement policies.
- Only 1.6% have DMARC policies that qualify as "BIMI ready."



Courtesy: BIMIRadar.com

Just **a fraction of a percent** of the domains the site is tracking have implemented BIMI, although that number is growing daily. Visit BIMIRadar.com to get the latest numbers, see which brands are implementing the specification, and dive further into BIMI readiness.

According to **Pathwire's VP of Deliverability and Product Strategy, Kate Nowrouzi**, some brands are afraid to enforce email authentication best practices. That's because they're more concerned with getting their own emails into the inbox rather than preventing brand impersonations.

"I was at a customer meeting with a bank and they're hesitant to have DKIM authentication because they felt even that was too new," Kate says. "In a lot of traditional organizations, there is some resistance to adopting any new protocol."

That resistance means many senders are failing to take advantage of the most effective way to stop email forgery: Domain-based Message Authentication, Reporting and Conformances, better known as DMARC.

"When DMARC came on board, the adoption rate at the beginning was very slow," Kate recalls. "People were afraid of emails being dropped or inadvertently sent to spam folders. BIMI is a motivation for brands to take DMARC seriously."

Kate Nowrouzi, Pathwire

A strong DMARC policy is a requirement for brands that want their logos to display next to emails. You can't have BIMI without implementing specific DMARC settings. The idea is, the potential for better branding would encourage the adoption of stronger email authentication.

The DMARC enforcement policy has a few possible applications: *"p=none"*, *"p=quarantine"*, and *"p=reject"*. This tells mailbox providers what to do with messages that fail authentication. **BIMI requires a DMARC policy of either quarantine or reject**. Kate Nowrouzi says too many brands were leaving the policy set to none, which didn't do much to help with authentication.

"It was supposed to be that way for maybe a week," says Kate. "But people put the DMARC policy in and it stayed at none. To realize the benefits of DMARC, you are supposed to go back and change that to quarantine or reject after a testing phase."

Problem 2: Brand logo control and verification

As you may know, brand logos in email inboxes are nothing new. Mailbox providers including Gmail and Microsoft Outlook sometimes make them part of the experience. However, email clients often have proprietary methods for acquiring these logos, which weren't always reliable.

For example, Gmail once relied on the now-defunct Google+ social network to find brand logos. Outlook uses Microsoft's Brand Cards, and Yahoo Mail had its own methods as well. Sometimes this meant an incorrect image showed up for the logo, including those of completely different brands. There are even instances where explicit content accidentally appeared as an inbox logo.

"I think there was a little bit of frustration for marketers," says Pathwire's Alex Rubin. "They'd ask 'Why is that logo showing next to my emails when it should be this one?' The mailbox providers would rather let the senders control their logos – as long as they are legitimate senders who can verify ownership of those logos."

Nothing makes a CMO's skin crawl as much as inconsistent branding. If they see an email with another brand's logo next to your email campaigns, it will be exponentially worse.

BIMI provides a way for brands to manage the logos used in email applications because mailbox providers will look for the record on the DNS and use whatever verified mark a brand chooses. It's also a **standardized way for email clients to identify the right logo**, which means less guesswork and fewer mistakes.

"So, BIMI seemed like a win-win situation," Alex adds. "It promotes DMARC authentication and lets brands control the logos that appear in the inbox."

Gmail support: BIMI's big break

Like DMARC, BIMI has faced hurdles around adoption. While it's certainly an interesting idea to many brands, there has been limited support from email clients. (Get the latest list of supporting providers from the BIMI Group.) Until recently, only Yahoo Mail, Verizon Media email services such as AOL, and Australian-based Fastmail supported BIMI.

That changed in July of 2021. After a year-long pilot program to test things out with select senders, Google announced it would officially roll out support for BIMI logos in Gmail. Alex Rubin called this a "big deal" and something the BIMI Group has been waiting for. **Matt Vernhout, Communications Chair at BIMI Group**, agrees.

"Gmail is the largest mailbox provider in the world. Supporting BIMI shows a commitment to driving adoption of DMARC and proper email authentication so you can get the reward of that logo in the end."

Matt Vernhout, BIMI Group

Gmail addresses likely make up a large portion of your subscribers. And, with the rise of Google Workspace (formerly G Suite) for business email, BIMI just became a worthwhile pursuit for both B2C and B2B brands.

At this point, Gmail supports BIMI at both the list and message view on the mobile app, but only at the message view in the Gmail web client. Google also has additional requirements around logos, and it still occasionally sources logos using other means. That's why you may notice local businesses with logos in the inbox. Matt thinks that could change.

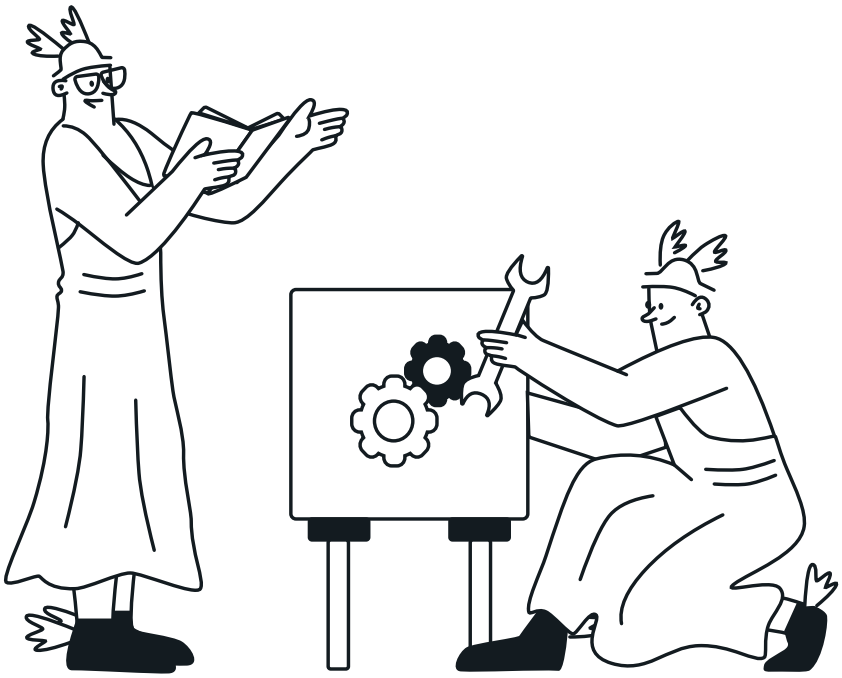
"If I were to get on my thinking cap and look two years into the future, Google will probably rely heavily on BIMI for identifying verified brand logos."

Here's why Google sees BIMI as an important part of security and branding in email marketing:

"BIMI provides benefits to the whole email ecosystem. By requiring strong authentication, users and email security systems can have increased confidence in the source of emails, and senders will be able to leverage their brand trust and provide their customers with a more immersive experience."

G Suite Security Features Announcement, July 21, 2020

Major financial institutions are among the early adopters of both BIMI and DMARC. Brands such as Bank of America and JPMorgan Chase see the value in both better branding and stronger email authentication.



PART 4

BIMI implementation: What to Expect

Email authentication is technical, and it can quickly become complicated. Even though the concept behind BIMI is quite simple, it's no exception. As the BIMI Group's Matt Vernhout explains, some of that complexity involves verifying ownership of your brand's logo.

"It's not just going to a website, punching in some information, and getting a cert," says Matt. "There's actual verification that gets done by a human to prove that you own the logo."

Sr. Email Marketing Manager Betsy Grondy worked to implement BIMI for Email on Acid brand while she was employed by the brand in 2021. Previously, she'd set up BIMI for a major tech company and a B2C ecommerce brand. Even though this wasn't her first time implementing BIMI, she still ran into some issues. Still, she understands exactly why.

"If it's easy to set up, it's probably easy to fake as well. And that would defeat the purpose of email authentication."

Betsy Grondy, formerly of Email on Acid

Betsy worked with Matt and others to troubleshoot problems and answer some of Email on Acid's questions. We spoke with them about what to expect and how to navigate roadblocks on the path to BIMI implementation.

Here are the steps you'll need to take to get a BIMI logo displaying for your brand:

Step 1. Find the right partners to help

While people like Matt and others connected to BIMI Group are happy to offer advice and resources to aid in set up and implementation, there may be others who'll need to get involved.

Most email marketers won't have direct access to the DNS for their sending domain. Even if you do, understanding how to format and publish a TXT record may not be your area of expertise.

For that reason, **you'll most likely need to reach out to the IT department for assistance**. While it may take a bit of explaining, IT professionals understand the risks of phishing and email security better than anyone.

Your email service provider (ESP) can also be a resource during BIMI implementation. You'll need to get your email authentication protocols in alignment, and your ESP might be the best place to get help with domain configuration. While ESPs sometimes use their own domains for authentication, you can often work with them to configure things as needed.

Roadblock: Existing email authentication setup

Betsy Grondy says BIMI might be easiest for brands that are starting from scratch with email authentication rather than augmenting it after it's in place. For some organizations, unraveling the complexities of server configuration and various TXT records may take a little longer.

Be sure to identify the right internal experts and find third-party partners who can guide you through it all.

"Email authentication is not always the IT department's forte or the typical email marketer's either," Betsy explains. "It's helpful to have that person who understands both sides and can bridge the gap."

Step 2: Identify your sending domain

Before you set up a BIMI record or update any of your other email authentication protocols, you'll need to know where they're meant to be published.

Many times, your sending domain is different from your brand's main domain. Organizations will use different subdomains as mail servers (i.e. mail.example.com or marketing.example.com). According to the BIMI Group's FAQs, BIMI records are designed to cascade down from one domain to subdomains. However, you can also publish specific BIMI records for different subdomains.

Roadblock: Sending domain confusion

When Betsy Grondy worked on Email on Acid's BIMI implementation, she found the brand actually was using its main domain to send email. This was also the domain employees used for their personal accounts at the company. And that caused some issues.

"Yahoo Mail wasn't recognizing us as a bulk mail sender," Betsy explains. "So, it wasn't implementing our BIMI record because our emails were coming from the main domain (hello@emailonacid.com) rather than a subdomain for email. They were classifying us the same as personal work emails."

In the end, a call to Yahoo explaining the situation helped rectify the situation. However, the bulk sender issue is another challenge to consider.

Roadblock: Bulk sender requirement

While it's true that BIMI could help standardize the process of sourcing logos in email and other applications, mailbox providers still have unique requirements.

For example, Yahoo wants to make sure it is only displaying BIMI logos for reputable senders. As part of that goal, it requires your brand to be a bulk sender. However, what exactly that means isn't clearly defined.

According to Marcel Becker, Senior Director of Product Management at Verizon Media, there's no precise send volume set as a threshold. Instead, it's part of a more complex algorithm Yahoo Mail uses when determining when to use BIMI logos.

Step 3: Email authentication alignment

As mentioned, one of BIMI's primary purposes is convincing more brands to adopt stronger DMARC enforcement policies. To get a BIMI logo to display, senders must:

- Have SPF and/or DKIM authentication in place.
- Have a DMARC policy set to either "p=quarantine" or "p=reject".
- Pass DMARC alignment (SPF or DKIM).

Those are the basic email authentication requirements for BIMI. However, some other factors may cause issues because they are considered "gaps" in DMARC enforcement.

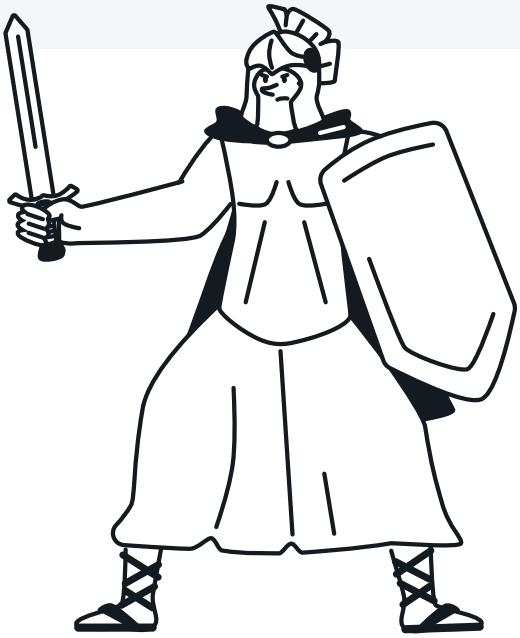
For example, if your DMARC policy includes the optional percentage tag it must be set to "pct=100", which is the default value. Anything less than that and BIMI won't work. Similarly, the "sp" tag, which is used to specify different policies for subdomains, may not be set to "sp=none".

At this point, DMARC alignment is the main requirement. That means you may not need both DKIM and SPF to qualify for BIMI. However, mailbox providers could change their policies in the future. The bottom line is, using both DKIM and SPF is a solid best practice.

Roadblock: Weak DMARC policies

One of the most common mistakes on the path to BIMI implementation is leaving your DMARC policy at "p=none". This means the sender's policy is telling receiving mail servers to take no action at all if authentication fails.

If you're just getting started with DMARC, be sure to use either quarantine or reject for your policy. If your policy is currently set to none, you'll need to augment DMARC to meet BIMI requirements.



Step 4: Create a BIMI logo

In addition to DMARC policy issues, BIMI Group Communications Chair, Matt Vernhout, says properly creating a BIMI logo is where many email marketers have questions. There are several specific requirements for BIMI logos.

- Logos must be trademarked.
- Logos must be SVG files (SVG P/S Tiny 1.2)
- The logo should be centered on a solid background.
- The image should be saved as a square but look good in a circular format.
- The file must be as small as possible (32kb or less is recommended)

SVG stands for scalable vector graphics. This file type is useful because it looks crisp and clear no matter how large or small the display. That makes BIMI logos flexible because they could be used in other situations beyond an icon for emails.

Roadblock: SVG file editing

The BIMI Group has specific requirements for SVG files used to create these logos. SVGs are XML files that describe an image, but additional information can be added to the metadata. That could allow BIMI records to be used in unintended ways, such as tracking user behavior. So, the group wants these particular SVG files to be as simple and secure as possible.

To make this happen, you'll need vector editing software like Adobe Illustrator to export your logo as an SVG Tiny 1.2. However, you'll also need to make some additional manual edits to remove certain SVG root elements ("x=" and "y="), which may not be possible within that software.

Even experienced graphic designers can get confused during this process because it isn't something they normally do. It may require a bit of back-and-forth to get the file right. Find information about editing SVGs for BIMI logos on the BIMI Group's website.

Step 5: Get a Verified Mark Certificate (VMC)

When Gmail started supporting BIMI, a new requirement emerged. Google wants to confirm brand ownership of logos. To do this, you must have a trademarked logo that is verified by a third party. The World Intellectual Property Organization (WIPO) has a search tool to help determine if your brand's logo is already trademarked.

A select group of certificate authorities (CAs) provides these so-called Verified Mark Certificates (VMCs). Once you're verified, you'll get a Privacy Enhanced Mail (PEM) file, which gets uploaded to your web server. As explained in Google Support documentation:

> *"Using a logo with a VMC helps prevent spammers and other malicious users from using brand logos they don't own. A logo that is a registered trademark is harder to spoof, or forge, because it's verified by the trademark organization."*

At this time, only Google is requiring VMCs for BIMI in Gmail. Verizon Media says while it does not require a VMC, it may be used to determine overall BIMI eligibility.

Roadblock: Additional costs

If you don't have a trademarked logo or a VMC, the process will take time and money. For enterprise organizations, it may not be a big deal. But for smaller brands, it may be cost-prohibitive.

So far, DigiCert and Entrust are the two entities authorized to provide VMCs, and they verify logos from trademark registration offices in a variety of nations as well as the European Union (EU). The cost ranges from around $900 to $1,000 for the first year (and they are valid for one year). It's unclear whether that will be a one-time setup fee or how much VMC renewal might cost. As more CAs enter the picture, competition could drive these prices down.

Matt Vernhout says the BIMI Group and Google are exploring ways to expand the standards so that logos without registered trademarks can acquire a VMC.

"Right now, there's not a great option for brands in government or the non-profit sector that don't necessarily need a trademarked logo," Matt explains. "BIMI Group is trying to find other ways to validate those logos."

Step 6: Publish your BIMI record

Once email authentication is aligned and you've got a verified logo in the correct format, it's time to build the actual BIMI record, which is added to your sending domain's DNS.

It will look something like this:

```
default._bimi.example.com in txt
"v=BIMI1; l=https://www.example.com/path/to/logo/example.svg;
a=https://www.example.com/path/to/vmc/VMC.pem;"
```

Here's how that breaks down:

- v= indicates the version of the TXT record, which should be BIMI1.
- l= the location/URL of your BIMI logo as an SVG file.
- a= the location/URL of your digital certificate to verify logo ownership.
  (If you do not have a VMC, it should read "a=self")

There's another value (s=), which indicates the use of selectors, similar to those connected to DKIM keys. A **BIMI selector is used to define other logos**. This could be useful when companies have multiple brands, but it is not a requirement.

Matt Vernhout explains that while multiple logos are possible with BIMI, and most mailbox providers support BIMI selectors, they are not yet widely supported by ESPs. He describes it as a "chicken and egg problem." Matt also points out that most brands require the use of only one logo.

Roadblock: TXT records typos

While a BIMI text record isn't overly complicated, it's still important to double-check everything and ensure you're using the correct syntax. Minor typos can result in BIMI authentication failure. To help avoid mistakes, there are BIMI generators available online.

Besides your BIMI record, you'll need to watch for possible mistakes in the DNS records of the other email authentication protocols as well. Don't forget, your emails need to pass DMARC validation (which includes SPF and DKIM) for deliverability and the display of BIMI logos.

If you're struggling to understand, create, or align email authentication records, there are experts who can help, including Red Sift cybersecurity and dmarcian.

Step 7: Verify BIMI is working

You're almost at the end of the path to BIMI implementation. After publishing a BIMI record to your DNS, the last step involves testing things out to see if everything is working as expected.

There are multiple tools that help verify whether BIMI is set up correctly. That includes the easy-to-use BIMI Inspector tool from BIMI Group. Plug in your sending domain and the tool will:

- Verify the presence of MX, SPF, DMARC, and BIMI records.
- Indicate any issues or warnings with those records.
  - Including a check for your VMC
- Verify you're using an acceptable SVG file for your logo.
- Show how your BIMI logo will look in dark mode.

If for some reason you want to turn off BIMI, perhaps because your brand's logo is changing and you don't have the right file yet, delete the BIMI TXT record on the DNS.

Roadblock: Patience required

It's entirely possible that you'll encounter one or more of the roadblocks we've mentioned. That means you'll need to retrace your steps and correct any issues.

If you don't have a trademarked logo, it could take weeks to take care of that. If you're starting from scratch with DMARC, that process may take some time as well. The more sources you have to configure, the more complex it is.

Even after you validate BIMI, it may take up to a week for some mailbox providers to start showing your logo. Just remember... patience is a virtue.

The BIMI Checklist

1 Find the right partners

Who has the expertise to help you manage technical difficulties?

ROADBLOCK: Existing email authentication
You may need to update and edit your DMARC policy and existing protocols.

2 Identify your sending domain

Does your organization use a specific subdomain as an email server?

ROADBLOCK: Bulk sender requirement
Some mailbox providers only approve BIMI logos for brands with high send volumes.

3 Email authentication alignment

Are you using SPF and DKIM with a DMARC policy of quarantine or reject?

ROADBLOCK: Weak DMARC policy
If your policy value is "p=none" you don't qualify for BIMI.

4 Create a BIMI logo

Is your BIMI logo in an SVG format and optimized for inbox display?

ROADBLOCK: SVG file editing
SVG files for BIMI must be in the P/S Tiny 1.2 format with a size less than 32kb.

5 Get a Verified Mark Certificate (VMC)

Have you worked with a certification authority to get your trademarked logo verified?

ROADBLOCK: Cost
A VMC will range in price from $900 to $1000 per mark for the first year.

6 Publish your BIMI record

Did you correctly format your BIMI TXT record and upload the certificate to the DNS?

ROADBLOCK: TXT record typos
Mistakes in any DNS records related to BIMI could cause authentication failures.

7 Verify BIMI is Working

How will you test to ensure you've set up BIMI correctly?

ROADBLOCK: Patience required
BIMI implementation isn't always easy. Retrace your steps if you have issues.

PART 5

Your brand and BIMI: What's next?

What does the future hold for BIMI? Matt Vernhout hopes Gmail support prompts more brands to look closely at their DMARC policies and pursue implementation. He also thinks other major email clients may follow Google's lead.

"I think now that Gmail supports it, we'll start seeing more interest in BIMI," Matt says. "We've already had developers reach out to say they're building it into apps. Obviously, we'd like to see the bigger mailbox providers like Microsoft and Apple come on board."

BIMI could also have uses beyond email. That's because it was designed to be used nearly anywhere you'd want a logo.

"I would love to see the Google Search team start putting BIMI logos in SERPs so you could see legit search results," adds Matt. "I'd love to see LinkedIn and Twitter start using BIMI on corporate pages so you can associate the domain with the corporate page and the logo gets auto-populated via BIMI."

While we wait to see what the future holds, Betsy Grondy thinks growing cybersecurity concerns and evolving consumer privacy regulations could drive BIMI adoption. From a branding perspective, competition could help as well.

In other words, if Pepsi and Ford get BIMI logos in their email campaigns, you can be sure Coke and Chevy will want it, too.

Is BIMI right for your brand?

The short answer is "yes". While this may not be the right time for your brand to work on BIMI implementation, the benefits of BIMI can help any brand build trust and fight phishing and spoofing attacks.

The brands that stand to benefit most from BIMI are those that are recognizable and at the highest risk of being impersonated. That includes financial institutions, consumer tech companies, eCommerce, and many other brands that require an online account.

But no matter how big or small your brand may be, email authentication is definitely worth the effort. Not only does email authentication help improve deliverability while protecting your customers and your brand, but it also protects email itself.

As marketers, we all want email to have a long life as a useful tool for everyone. If we let spammers and scammers rule the inbox, people may abandon it for good. The more brands and mailbox providers there are with strong email authentication practices, the better off we'll all be.

PART 6

How Pathwire can help

Email authentication is just one factor connected to deliverability. Pathwire designed its growing suite of deliverability apps and services to help you reach more inboxes with connected experiences.

From email validations to advanced deliverability insights, marketers use our tools to proactively address issues before hitting send. Trust Pathwire's team of experts to guide you through the complexities of getting your messages to the right people at the right time.

PART 7

Acknowledgments

Special thanks to the email marketing experts and organizations that contributed to this content.

Alex Rubin
Sr. Director, Strategic Partnerships, Pathwire

While at Return Path, Alex was an original member of the BIMI Group. He currently leads Pathwire's partner team where he is helping companies empower their email strategies.

Kate Nowrouzi
VP Deliverability and Product Strategy, Pathwire

Kate is an email industry veteran with deliverability and compliance expertise. She is an active voice in the anti-spam community as well as an advocate for inclusion, diversity, and STEM education.

Matt Vernhout
Communications Chair, BIMI Group

In addition to his work with BIMI Group, Matt is VP of Deliverability, North America at Netcore Cloud. He also runs the website EmailKarma.net, which offers email marketing news and knowledge.

Betsy Grondy
Sr. Email Marketer

Betsy is an accomplished email marketer who has led global email strategy and execution for B2B and B2C brands, including Email on Acid.

Marcel Becker
Sr. Director Product Management, Verizon Media Group

Marcel is a self-described "email nerd" and BIMI Group member. At Verizon Media Group, he focuses on requirements and business relationships around deliverability, anti-abuse, and email security.

Red Sift

The team at Red Sift provides cybersecurity technology for enterprise organizations. That includes the award-winning, cloud-based application OnDMARC, which features automated email authentication setup. The company also tracks "BIMI readiness" at BIMIRadar.com.

Pathwire empowers 100,000 paying customers around the world to solve complex communication problems. Through its powerful email API and intuitive email marketing solutions, Pathwire delivers over 250 billion emails a year for companies like DHL, Wikipedia, Toast, Lyft, and Microsoft.

The company provides reliable, cloud-native infrastructure, local expertise, and smart solutions based on machine learning so companies can more easily reach their customers and build connected experiences. Pathwire has offices worldwide including in the UK, Spain, France, Germany, and the US.

For more information, please visit **www.pathwire.com**.