

Legal Alerts

Understanding BIMI: Protecting Your Brand in the Inbox

12.12.25 04.30.26

With the constant stream of email spoofing and phishing attempts in consumer's inboxes, recipients increasingly struggle to distinguish legitimate emails from fraudulent ones. Brand Indicators for Message Identification (BIMI) can help organizations display a verified brand logo directly in recipients' inboxes in an effort to provide immediate visual confirmation that the email is authentic.

Why BIMI Matters for Your Brand

BIMI can offer a safer and more intuitive email experience. When a verified logo appears next to a new email message, users can use that to more quickly identify legitimate messages, reducing the chance that trusted communications are flagged as spam or "suspected phishing." For businesses, BIMI can promote trust, increase brand recognition and improve engagement by helping emails stand out visually.

BIMI Certificates: Verified Mark Certificate vs. Common Mark Certificate

BIMI works hand-in-hand with certain existing email security tools, especially the Domain-based Message Authentication, Reporting & Conformance (DMARC). BIMI was introduced to encourage widespread DMARC adoption by offering brands a clear incentive where once an organization authenticates its emails at the highest level (with a DMARC policy of quarantine or reject), participating mailbox providers may display the organization's verified logo directly in recipients' inboxes.

To enable this display, most major email providers require organizations to obtain a Verified Mark Certificate (VMC). A VMC is a digital certificate that confirms (1) the logo is protected by a valid trademark registration from a recognized trademark office (e.g., the United States Patent and Trademark Office), and (2) the sending domain has passed the necessary authentication checks. For companies with registered trademarks, a VMC is the most widely supported path and remains a strong choice for BIMI implementation.

Organizations that do not yet have trademark protection may pursue a Common Mark Certificate (CMC) by demonstrating at least 12 months of consistent use of a particular logo. However, many mailbox providers do not recognize CMCs, so their effectiveness can be limited. Both VMC and CMC routes for BIMI can require annual fees, specific scalable vector graphic (SVG) logo files and additional requirements depending on the provider.

Trademark & Branding Considerations

Since BIMI uses an organization's logo as a verified trust signal, trademark protection becomes a key requirement. To obtain a VMC, a company must own a registered trademark for the exact logo it plans to display. The BIMI process thus is also an opportunity to evaluate the robustness of brand protection, including verifying current logo registrations, determining whether additional filings are needed and addressing any logo updates that may require new trademark applications. This in turn can add value to a company's IP portfolio by strengthening its rights and filings.

BIMI Implementation Checklist

Establish Prerequisites

- Confirm that your logo is protected by a registered trademark with a recognized trademark office (required for a VMC).
- Ensure your domain is fully DMARC-compliant with a quarantine or reject policy in place.
- Verify domain ownership and confirm sender policy framework (SPF) and domain keys identified mail (DKIM) records are properly configured.

Select & Obtain the Appropriate Certificate

- Determine whether a VMC or CMC is appropriate.
- Plan for annual certificate costs.
- Engage an approved certificate authority to complete the application process.

Host Required Files

- Upload the VMC or CMC digital certificate to a secure, encrypted server to ensure it can be safely accessed during the BIMI verification process.
- Upload your BIMI-compliant SVG logo to a secure server.
- Confirm that the SVG used in your BIMI record matches the logo referenced in the certificate.

Publish the BIMI Record

- Create the BIMI TXT record - this is a special entry in a domain's DNS that tells email providers where to find your verified logo and certificate.
- Publish the BIMI TXT record - this allows mailbox providers to locate and display your logo when your emails pass authentication checks.

Validate & Monitor

- Test any configurations using a BIMI record-checking tool.
- Review DMARC reports on a regular basis.
- Monitor logo display across participating mailbox providers.

Looking Ahead

While BIMi implementation ultimately depends on both technical configuration and email provider adoption, partnering with experienced legal professionals can help ensure that your trademark assets, branding materials and authentication practices are aligned with emerging standards. Proactive steps for trademark protection and brand recognition can in turn help customer communication and distinguish companies from the competition.

The information above involves complex legal considerations and is provided for general informational purposes only. It does not constitute legal advice. For guidance on specific legal matters, please contact your attorney.

Authored by

[Claire F. Hawkins](#)

[Principal|Seattle](#)

[206.816.1301](tel:206.816.1301) claire.hawkins@foster.com

[Kenzie Kinsella](#)

[Associate|Seattle](#)

[206.447.8983](tel:206.447.8983) kenzie.kinsella@foster.com

Related Areas

- [Copyright, Trademark, Trade Secret & More](#)
- [Intellectual Property, Privacy & Technology](#)
- [Privacy, Data Protection & Cybersecurity](#)