# DMARC and BIMI

A Refresher for 2023 and Beyond

# Todd Herr

**Technical Director, Standards and Ecosystem
Valimail**

todd.herr@valimail.com

# Agenda

- My Background

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

- BIMI (Brand Indicators for Message Identification)

- Why you MUST do DMARC

- Hurdles to BIMI adoption and the way forward

- Audience Q&A

# A Little Bit About Me

- Well over twenty years experience in email, including
  - Postmaster, Time Warner Cable/RoadRunner
  - Return Path (ISP liaison, data trades, FBLs)
  - SparkPost (Deliverability and Tools)
  - Current co-editor for IETF DMARCbis effort (updates to DMARC RFC)
  - Current committee co-chair for AuthIndicators Working Group (BIMI standards development)
  - Current co-chair, M3AAWG Technical Messaging subcommittee

# DMARC – Prevent Spoofing

- The intent of DMARC is to prevent spoofing of the domain in the visible From: header

- DMARC is about authenticated identities; it's a best practice, but by itself it doesn't mean you're a good sender.

- Authentication gets you the deliverability you deserve.

# DMARC Primer

- For domain owners, DMARC
  - Announces authentication practices
  - Provides opportunity to request handling for messages that fail authentication checks (p=)
  - Allows domain owners to collect data on use of its domain (rua=)
- For mailbox providers, DMARC
  - Allows validation of use of the domain in the visible From: header
  - Provides one or more anchors (authenticated identities) for reputation scores

# DMARC Primer

- DMARC relies on two underlying authentication protocols
  - SPF – A domain owner can authorize servers and networks to use its domain in the Return-Path header (a.k.a., "bounce domain", "mail from domain", "envelope sender")
  - DKIM – A domain owner can take responsibility for a message by inserting two cryptographic hashes in a header, along with information on how to validate them. If the hashes validate at the receiving end, the receiver knows the message was unchanged.

# DMARC Primer

- Domain alignment required
  - Domains align when they have the same organizational domain (relaxed) or when they're identical (strict)
  - Organizational domain (a.k.a., "apex domain") is the domain that is registered by an entity wishing to establish an online presence.
- DMARC pass requires either:
  - SPF pass plus SPF domain aligned with From: domain
  - DKIM pass plus DKIM domain aligned with From: domain
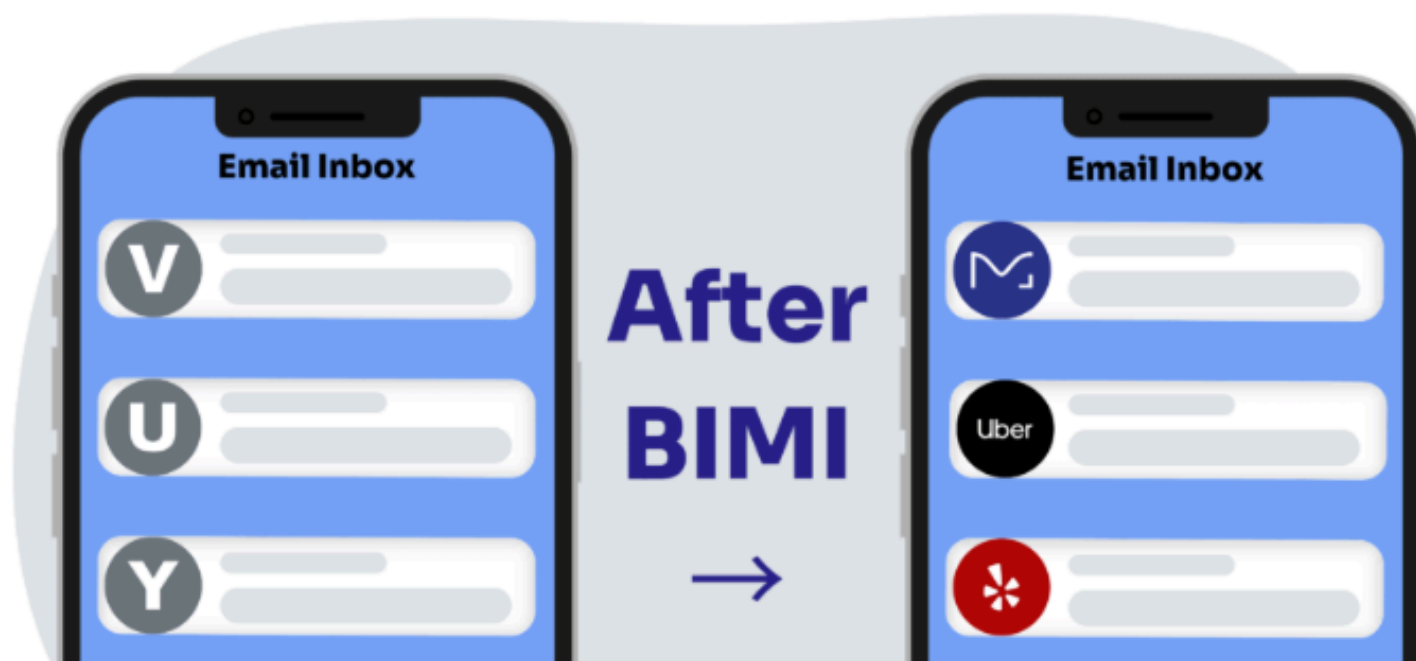
# DMARC Primer

- Basic record
  - "v=DMARC1; p=none; rua=mailto:reports@foo.com"
- Policy choices (p= tag)
  - none (apply no special treatment if DMARC fails)
  - quarantine (route to spam folder if DMARC fails)
  - reject (reject or bounce if DMARC fails)
- Policy choices are *requests*
  - No requirement that mailbox provider honor them
  - Some treat p=reject as p=quarantine, for example

# DMARC Primer

- Aggregate Reports
  - Daily summary data from participating mailbox providers on use of your domain
  - What sources passed SPF, DKIM, and/or DMARC, and which failed
  - Intended for addressing shortcomings in authentication practices before domain owner ramps up to *quarantine* or *reject*.
  - At Valimail, we refer to quarantine or reject as "at enforcement"

# BIMI – What Is It?

- A still developing protocol to allow domain or brand owners to specify an image or logo to be shown next to messages in recipients' Inboxes.

# BIMI – Who Will See My Logo?

**Supports BIMI**

Apple

CLOUDMARK
A PROOFPOINT COMPANY

Fastmail

Google

LA POSTE

onet POCZTA

yahoo!

ZONE

**Considering BIMI**

at mail

BT

COMCAST

QUALITIA

SEZNAM.CZ

WEB.DE GMX

YAHOO! JAPAN

**Does not support BIMI**

Microsoft

# BIMI – What's Required?

- Organizational Domain and From: Domain (if different) MUST have DMARC policies at enforcement
  - BIMI is intended to be the carrot to DMARC's stick
- Logo used MUST be trademarked
  - Format is SVG Tiny Portable/Secure (SVG Tiny PS)
- Verified Mark Certificate (VMC) must be obtained from a third party (Digicert and Entrust for now)
  - VMC is attestation that organization using logo has rights to do so

# BIMI – How Do I Do It?

- After you've met the pre-requisites, it's just one DNS record:

"v=BIMI1; a=https://full/path/to/VMC.pem; l=https://full/path/to/logo/file.svg"

- BIMI supports selectors, so multiple logos are possible
  - Multiple domains allowed per VMC
  - Only one logo allowed per VMC

# BIMI – What's In It For Me?

- BIMI makes your email stand out in the Inbox
  - Brand recognition *should* drive more engagement
- The DMARC work to qualify for BIMI means all email using your company's domain is authenticated
  - Opportunity for Marketing to work with CISO and IT
    - CISO and IT want to guard against spoofing of domain
    - Marketing wants the logo showing up everywhere
- Is there *ever* a bad time to get your logo in front of customers and potential customers?

# Why You MUST Do DMARC

- October 3, 2023 Google and Yahoo announced new policies for bulk senders to take effect in February, 2024 ("No Auth, No Entry"), including
  - SPF must be in place for Return-Path domain
  - Mail must be DKIM signed
  - From: domain must have DMARC policy record (p=none)
  - SPF or DKIM (preferably DKIM) domain must align with From: domain
- https://www.valimail.com/blog/the-new-requirements-for-email-delivery-at-gmail/

# Hurdles to BIMI Adoption

- DMARC at enforcement
  - Not changing. BIMI is an incentive to do DMARC.
  - Mailbox providers want DMARC because authentication is an anchor for reputation
- Trademarked Logos
  - Not all organizations have trademarked logos
  - Some orgs' trademarked logos don't fit or look good in BIMI
- Difficult to demonstrate value
  - Engagement metrics aren't what they used to be

# Hurdles to BIMI Adoption

- Inconsistent User Experience
  - Gmail, for example, shows logo in folder list in mobile, but only after message opened on web
- Interoperability challenges
  - Mail sent to Gmail, viewed in Gmail client, shows logo
  - Mail sent to iCloud, viewed in Apple Mail client, shows logo
  - Mail sent to Gmail, viewed in Apple Mail client, **does not** show logo at this time

# Solutions on the Horizon?

- Trademarked Logos
  - Current spec defines two types of non-trademarked logos – Modified Mark and Prior Use Mark
  - Mailbox providers exploring ways to support these
- Difficult to demonstrate value
  - Track conversions rather than opens?
  - There's never a bad time to get your logo in front of customers
- Interoperability/UX Challenges
  - In-protocol solutions defined
  - Mailbox providers have to see benefit to implementing

# Time for Q&A

# Resources

- BIMI – AuthIndicators Working Group – https://bimigroup.org/

- DMARC – IETF DMARC Working Group - https://datatracker.ietf.org/wg/dmarc/about/

- M3AAWG – Best practices for sending and email authentication – https://m3aawg.org/

- Valimail – We can help you solve your DMARC and BIMI implementation challenges – https://valimail.com/