Return Path

DMARC

Phishing attacks continue to be one of the top Internet security threats, costing companies and individuals billions of dollars every year. Enter DMARC.

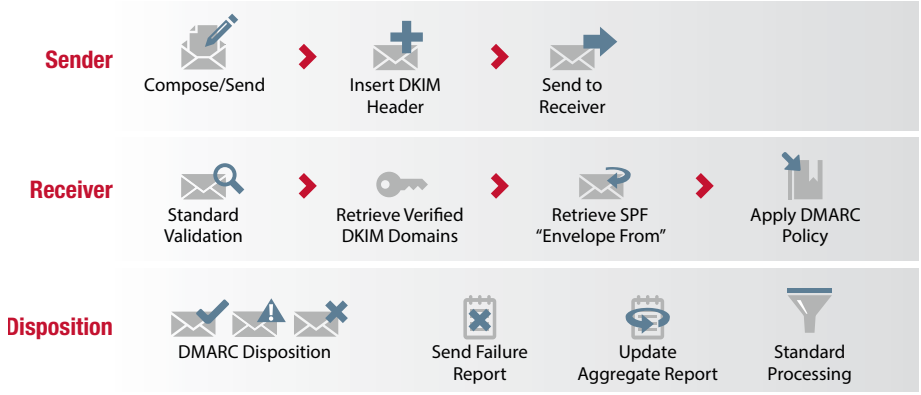
"Synacor enables our ISP customers to offer their end-consumers an email environment everyone can trust. The adoption and use of DMARC plays a key role in that ability, providing a mechanism that can be used to protect mailboxes from many domain phishing attacks."

- Eric Toczek,
Director of Email, Synacor, Inc.

Prevent Messaging Abuse and Fraud

New DMARC specification standardizes email authentication and restores trust in the email channel.

The Domain-based Message Authentication, Reporting & Conformation (DMARC) specification standardizes how email receivers perform authentication-based policy using the widely-deployed SPF and DKIM mechanisms. This allows senders to broadcast their authentication practices to any email receiver implementing DMARC.



Return Path

Did you know?

- Sender adoption of email authentication standards (SPF and/or DKIM) is estimated at over 75%.
- 35% of messages received by large mailbox providers are from domains protected by DMARC.
- 50% more sending domains published DMARC records over the course of 2014.

- Source: Online Trust Alliance

Benefits to *Mailbox* Providers (a.k.a., Receivers)

In addition to protecting a sender's end customers from fraudulent and often malicious email threats, receivers stand to benefit greatly from the DMARC standard.

Some of these benefits include the ability to:

- Gain knowledge into how to handle un-authenticated and failing email.
- Provide feedback (aggregated and forensic reports) to domain owners on email that does not pass authentication.
- Reduce domain spoofing and the impact of phishing and fraudulent email messages delivered to end-users.
- Decrease spam and improve ability to deliver legitimate mail to end-users.

5-Step Receiver Implementation Process

1. **Extract Sender Domain (RFC5322.From field):** This is the domain to be evaluated by DMARC. Messages with multiple RFC5322. From identifiers will be rejected by DMARC.
2. **Determine Domain Existence:** Before undertaking a DMARC evaluation, receivers should verify whether or not the DNS domain found in the RFC5322. From field actually exists. If it is determined that the domain does not exist, the message should be rejected
3. **Establish Handling Policy:** There are 6 sub-components to this step which include:
   a. Extract the RFC5322. From domain from the message.
   b. Query the DNS for a DMARC policy record and continue if one is found.
   c. Perform DKIM signature verification checks. Results from this step must include the value of the "d=" tag from all DKIM signatures that were successfully validated.
   d. Perform SPF validation checks. The results of this step

Return Path

Learn more about DMARC and other Email Fraud Protection solutions at www.returnpath.com/stopemailfraud

must include the domain name from the RFC5321. MailFrom domain if SPF evaluation returned a "pass" result.

e. Conduct identifier alignment checks to verify if Authenticated Identifiers (RFC5322. From, DKIM signature, and RFC5321.MailFrom) fall into alignment. If one or more of the Authenticated Identifiers align with the RFC5322.From domain, the message is considered to pass a DMARC check. All other conditions are considered to fail the DMARC check.

f. Apply policy based on DMARC record. Emails that fail DMARC check are disposed of in accordance with DMARC policy of the domain owner.

4. **Apply Message Sampling Rate:** If the "pct" tag is present within the DMARC policy, receivers must not enact the requested policy on more than the stated percent of the total affected messages.
5. **Store Results of DMARC Processing:** The results of receiver-based DMARC processing should be stored for eventual presentation back to the domain owner in the form of aggregate feedback reports.

Return Path Email Fraud Protection Solutions

To help both senders and receivers take advantage of DMARC quickly and easily, Return Path has already integrated DMARC policy standards into Email Fraud Protection. Domain Protect for Mailbox Providers can automatically analyze DMARC data provided by mailbox providers and provide real-time reporting and alerting back to domain owners, empowering them with the ability to make informed policy statements and reduce phishing attacks upon their end-users. In exchange for providing DMARC and email authentication data, our mailbox provider partners have free access to the Return Path Trusted Sender Registry, a registry of trusted senders whose email authentication practices have been verified by Return Path. Return Path also offers several free tools to help create and

validate DMARC records and troubleshoot authentication.

About Return Path

The Return Path solutions are fueled by the world's most powerful email data platform. We work across all parties — mailbox providers, email service providers, application developers and individual email users — to provide a more transparent picture of the information landscape, helping brands make more effective, meaningful and profitable connections with customers.

For more information, contact us today or use one of the email addresses to the left to get in touch.

Global Offices

USA (Corporate Headquarters)
rpinfo@returnpath.com

Australia
rpinfo-australia@returnpath.com

Brazil
rpinfo-brazil@returnpath.com

Canada
rpinfo-canada@returnpath.com

France
rpinfo-france@returnpath.com

Germany
rpinfo-germany@returnpath.com

United Kingdom
rpinfo-uk@returnpath.com