GROWTH CAB | VERSION 1 | REVIEWED 10 SEPTEMBER 2026

Deliverability diagnosis: worked example

Simulated, not a result. Synthetic header facts. Do not execute DNS or sending changes from this example without diagnosing your own environment.

Illustrative incident, not a client case or a deliverability guarantee. Do not execute DNS or sending changes from this example without diagnosing your own environment.

Observation and scope

A fictional team reports that replies declined after moving one campaign to a new sending service. There is no reliable inbox-placement measurement. Campaign copy, audience and infrastructure changed together, so reply rate alone cannot isolate the cause.

SPF pass
bounce.vendor.example

DKIM none
no signature on the sample

DMARC fail
From sender.example, no alignment

1 retest
authorized message, same path

Evidence ledger

A received test-message header shows SPF=pass for bounce.vendor.example, DKIM=none and DMARC=fail for visible From sender.example. These are synthetic header facts. The different organizational domains do not align. A separate campaign message received an SMTP rejection; its exact enhanced status code, timestamp and destination provider must be inspected rather than inferred from the reply-rate decline.

Interpretation

The successful SPF check authenticates the envelope sender in this example. It does not align that identity with the visible From domain. With no aligned DKIM pass either, the sample fails DMARC. This is an authentication finding for that message, not proof of the cause of every missing reply or a diagnosis of all providers.

Bounded action

The messaging administrator inventories legitimate senders and follows the service's documented setup for signing with the correct domain and aligning the relevant identities. Preserve existing legitimate senders and validate proposed DNS changes before publishing. Do not weaken DMARC policy, rotate domains or increase volume to conceal the failure.

Retest and decision

Send only an authorized diagnostic message through the same affected path. Inspect the received Authentication-Results header and actual SMTP outcome. If aligned authentication passes, mark this defect corrected for the tested path. If it still fails, compare the service, signing domain, selector and DNS state; do not change copy to fix authentication.

Then assess provider-specific rejections, complaints, recipient quality and sending changes independently. Authentication passing is not evidence that a message reached the inbox, that reputation recovered or that prospects will reply. Record unknowns rather than replacing them with an arbitrary score.

Official references

Google's sender requirements distinguish personal Gmail recipients and sender-volume categories. Use the applicable requirements, not a threshold copied across all providers. Reference: https://support.google.com/mail/answer/81126?hl=en

Microsoft explains the separate roles of SPF, DKIM, DMARC and composite authentication. Reference: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about

Reusable incident record

Record provider; UTC time window; sending service; visible From domain; envelope domain; DKIM signing domain; message/SMTP evidence location; observation; hypothesis; approved owner/action; retest result; remaining unknowns. Keep full private headers in an access-controlled location, not a public worksheet.

Source page: https://www.growthcab.com/email-deliverability-consultant