

— FIELD MANUAL · THE COLD EMAIL OPERATOR'S REFERENCE

# The Deliverability Cheat Sheet.

Twenty field-tested principles for keeping mailboxes alive, copy fresh, and reply rates compounding. Distilled from consulting calls with operators sending tens of thousands to three million emails a day.

---

**20**

PRINCIPLES

---

**3M**

EMAILS / DAY TESTED

---

**100%**

FIELD VERIFIED

AUTHORED BY

**Tony Baltodano** · Co-Founder, Mission Inbox

## 20 PRINCIPLES, 1 ACTION SHEET

# Index of Principles.

Each principle is its own page. Read in order for the full mental model, or jump straight to the page that matches the fire you're putting out today.

|           |                                       |              |           |                                     |              |
|-----------|---------------------------------------|--------------|-----------|-------------------------------------|--------------|
| <b>01</b> | <b>Copy Fatigue Is the #1 Killer</b>  | <b>P. 03</b> | <b>11</b> | <b>Domain Diversification</b>       | <b>P. 13</b> |
| <b>02</b> | <b>Spintax Alone Is Not Enough</b>    | <b>P. 04</b> | <b>12</b> | <b>Domain Naming &amp; TLDs</b>     | <b>P. 14</b> |
| <b>03</b> | <b>Sender Name Randomization</b>      | <b>P. 05</b> | <b>13</b> | <b>Dedicated IP Reputation</b>      | <b>P. 15</b> |
| <b>04</b> | <b>Signature Hygiene</b>              | <b>P. 06</b> | <b>14</b> | <b>Stop Tracking Opens</b>          | <b>P. 16</b> |
| <b>05</b> | <b>Mailbox Rotation Beats Warm-Up</b> | <b>P. 07</b> | <b>15</b> | <b>Subject Line Variation</b>       | <b>P. 17</b> |
| <b>06</b> | <b>Zombie Mailbox Quarantine</b>      | <b>P. 08</b> | <b>16</b> | <b>Suppression Lists</b>            | <b>P. 18</b> |
| <b>07</b> | <b>Redirects Kill You at Scale</b>    | <b>P. 09</b> | <b>17</b> | <b>Placement Testing</b>            | <b>P. 19</b> |
| <b>08</b> | <b>If You Scrape Google Maps</b>      | <b>P. 10</b> | <b>18</b> | <b>The Pre-Burn Window</b>          | <b>P. 20</b> |
| <b>09</b> | <b>Google vs. Enterprise Gateways</b> | <b>P. 11</b> | <b>19</b> | <b>The Warm-Up Reality</b>          | <b>P. 21</b> |
| <b>10</b> | <b>Personal Gmail Burn Rate</b>       | <b>P. 12</b> | <b>20</b> | <b>When Things Go Wrong</b>         | <b>P. 22</b> |
|           |                                       |              | <b>★</b>  | <b>Quick-Reference Action Sheet</b> | <b>P. 23</b> |

## PRINCIPLE 01 · COPY FATIGUE

## Copy Fatigue Is the #1 Killer.

Mailboxes don't usually die from "bad infrastructure." They die because the same copy gets sent thousands of times until mailbox providers fingerprint the structure and start filtering it. Once a mailbox is contaminated by burned copy, no warm-up will save it.

## FIELD EVIDENCE

- One client sent **44k+ emails** with essentially the same template before reply rates collapsed.
- Another saw reply rate halve (**3.51% to 1.8%**) when volume went from 102k to 255k with identical copy and ICP.
- A high-volume client sending **3M emails/day** on a single offer has zero copy issues: variations are generated programmatically and rotated constantly.

## WHY IT WORKS THIS WAY

ESPs (email service providers) don't penalize "an email." They penalize a fingerprint: a structural signature of sentence patterns, phrasing, opening lines, CTA structure, signature format. Spintax alone (changing "Hi" to "Hello") doesn't change the fingerprint. What changes the fingerprint is structural variation.

## THE FIX: ACTION SEQUENCE

- 01** Take your base copy that's working (or used to work).
- 02** Drop it into Claude: "Create 5 structurally different variations. Keep the offer identical. Change sentence structure, count, phrasing, and opening hook."
- 03** Apply spintax on top of each of those 5 variations.
- 04** Build a 20-variation pool of subject lines: all lowercase, max two words, no spam words.
- 05** Rotate variants every ~5,000 sends per mailbox before introducing the next batch.

## PRINCIPLE 02 · SPINTAX

## Spintax Alone Is Not Enough.

Spintax changes wording. Structural variation changes the shape of the email. ESPs identify the shape, not the wording.

## THE HIERARCHY OF VARIATION

## LEVEL 01: WEAKEST

Spintax on greetings and closings only. Almost useless at scale.

## LEVEL 02

Spintax on the body. Better, but still the same structural fingerprint.

## LEVEL 03

Multiple structural variants, each with its own spintax. Strong defense.

## LEVEL 04: WHAT 3M/DAY OPERATORS RUN

Multiple structural variants + multiple subject line pools + sender name randomization + signature variation. Compounds into billions of unique permutations.

## THE MATH

**5 structural variants x spintax on each x 20 subject line variants x randomized sender names = effectively billions of unique combinations.** ESPs can fingerprint and kill one variant; you still have everything else firing.

Structurally, the emails **have to be different**. That is the most important thing.

## PRINCIPLE 03 · SENDER NAMES

# Sender Names Buy You 2-3 Extra Weeks.

Don't reuse the same first/last name across hundreds of mailboxes. Randomize fully: every mailbox gets a unique sender identity.

**2-3wk**

ADDED MAILBOX LIFESPAN

**1:1**

NAMES PER MAILBOX

**15**

COMMON MISTAKE (TOO FEW)

## WHY IT WORKS

When sequencer signatures auto-populate from the mailbox sender name, every email gets a unique signature footprint. This breaks the pattern mailbox providers use to group "this sender is the same operator running the same campaign across 500 inboxes."

## WHAT CHANGES

**Mailbox longevity, not reply rate.** A mailbox that would have lasted 3 weeks now lasts 5 to 6 weeks before reply rate degrades. The reply rate ceiling stays the same, but the mailbox squeezes more total revenue out before it has to be rotated.

## COMMON MISTAKE

Operators using ~15 names across thousands of inboxes. Way too few. Filters group these instantly. If you have 500 mailboxes, you need 500 unique sender names. No exceptions.

## THE RULE OF THUMB

- One unique sender name per mailbox. Generated programmatically, not hand-picked.
- Pull from a wide pool: combine first names and last names from large lists for thousands of unique permutations.
- Pair sender name randomization with signature randomization (job title, formatting).

## PRINCIPLE 04 · SIGNATURE HYGIENE

## No Hyperlinked Company Names.

Don't put your company name as a hyperlink, or as a URL, in the signature. Even when typed as plain text, recipient email clients automatically render any .com string as a clickable URL, which is a known spam trigger at volume.

**DON'T**

- ✗ companyname.com (auto-hyperlinks)
- ✗ Clickable company name
- ✗ Tracking URL in signature
- ✗ Same signature across all mailboxes

**DO**

- ✓ "Company Name" as plain text only
- ✓ No URL in signature at all
- ✓ Vary job title across mailboxes
- ✓ Mix phone presence on/off

## VARIABLES TO RANDOMIZE

**Job title:** Founder, Cofounder, Head of Growth, Director, Partner, Account Executive, etc. Rotate widely so no two mailboxes share the same title.

**Company name presentation:** capitalization, spacing, abbreviations. Same brand, multiple visual treatments across mailboxes.

**THE PLAIN-TEXT TRAP**

Even if you type the company name with no URL, the recipient's email client (Gmail, Outlook, Apple Mail) automatically detects .com and renders it as a clickable link in the displayed email. Strip the .com entirely. Brand name as a word, nothing more.

## PRINCIPLE 05 · ROTATION

## Rotation Beats Warm-Up.

Once a mailbox starts hitting spam, no amount of warm-up will rehabilitate it. Warm-up only works before the mailbox burns. After burn, it's a zombie, and zombies infect healthy mailboxes nearby.

## THE 3X INFRASTRUCTURE RULE

Buy **3x the infrastructure** you need at peak volume. The math:

**1x**

ACTIVE SENDING

**1x**

WARMING UP NEXT

**1x**

COOLING / REPLACING

## THE ROTATION CADENCE

## WEEK 1-3

Run a campaign on the active mailbox batch.

## WEEK 4

Move that batch to warm-up. Rotate in the fresh batch from the warm-up pool.

## ONGOING

Rinse and repeat. The mailbox doesn't have to be dead to rotate it out. Rotate before it burns, not after.

## KEY INSIGHT

Most operators wait too long. They rotate when reply rates have already collapsed and the mailbox is contaminated. **The right time to rotate is when the mailbox is still healthy**, before any signal of decline. That's how you preserve the asset for a future life cycle.

## PRINCIPLE 06 · QUARANTINE

## Zombie Mailbox Quarantine.

If one mailbox on a domain is hitting spam, assume all mailboxes on that domain are hitting spam. Domain reputation is shared across mailboxes, no exceptions.

**Treat a burned mailbox like a zombie. Healthy mailboxes sending the same content next to a zombie get infected.**

## THE QUICK TEST

- 01 Pick one mailbox per domain.
- 02 Run it through a placement test (managed seed network or manual seed inbox).
- 03 If it lands in spam, kill all mailboxes on that domain.
- 04 Don't try to save them. Don't pause and warm them up. Domain is done.

## THE CANCELLATION ORDER MATTERS

Step 1: Cancel the subscription on the mailbox provider's dashboard. Step 2: Then delete the mailbox from your sequencer.

If you reverse the order, you keep getting billed for mailboxes that no longer exist in your workflow. This mistake costs operators thousands per month in zombie billing.

## THE SHARED REPUTATION REALITY

A domain has a single reputation score with each ESP. Every mailbox on that domain inherits it. Even if one mailbox has only sent 50 emails and another has sent 5,000, both share the same fate when the domain goes into spam. **Diagnose at the domain level, not the mailbox level.**

## PRINCIPLE 07 · THE REDIRECT TRAP

## Redirects Kill You Above 10k/Day.

The standard practice since 2018 has been to buy lookalike domains and redirect them to the client's actual website. It worked for years. It no longer scales: at meaningful volume, redirected lookalike domains get tracked and blacklisted.

### FIELD EVIDENCE

A client had 25 different lookalike domains all redirecting to the same client website. The ESP that blacklisted them said exactly that as the reason. Removing the redirects fixed deliverability within days. No other change was made.

### THE THRESHOLD MAP

| DAILY VOLUME  | REDIRECT STATUS             | WHAT TO DO                                                                         |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| <10k / day    | Lookalike to client site OK | Standard practice. Monitor reply rate weekly.                                      |
| 10k-50k / day | Domain masking preferred    | Mask the redirect chain to reduce ESP visibility.                                  |
| 50k+ / day    | No domain at all is better  | Unless you can build a unique landing page per domain, drop the redirect entirely. |

### WHY "NO DOMAIN" WINS AT SCALE

At 50k+ per day, having a redirect, even a masked one, is worse than having nothing. Building a unique landing page for every individual domain in your sending pool would solve it, but the cost and maintenance burden almost never justifies the marginal lift. **Most operators are better off letting the offer live entirely in the email body** and skipping the landing page altogether.

**Notice how more cold email senders now have no redirect at all on their domain? That's intentional. It's the new best practice at scale.**

## PRINCIPLE 08 · PERSONAL ADDRESS REALITY

## If You Scrape Google Maps, Read This.

A lot of local businesses list a personal email address (Gmail, Hotmail, Outlook, Yahoo, iCloud) as their public inquiry contact. Even when your scraping is legitimate and the recipients are real people, sending to personal addresses is a completely different beast than sending to business domains.

## THE SCOPE OF THIS RULE

This principle matters most for operators **scraping data from Google Maps** or similar sources where local SMB contact info is exposed. The mailbox listed publicly is rarely a real Google Workspace or O365 business mailbox. It's a personal account the business owner uses for everything. That changes the deliverability math.

## STRIP OR AVOID

- ✗ @outlook.com / @hotmail.com / @live.com
- ✗ @yahoo.com
- ✗ @icloud.com / @me.com
- ✗ @aol.com and other legacy free providers

## SEND TO (HEALTHY)

- ✓ @gmail.com (personal Gmail): see Principle 10 for caveats
- ✓ Google Workspace business addresses
- ✓ O365 / custom-domain corporate addresses

## WHY THE INBOX FOLDER IS ALMOST IMPOSSIBLE HERE

Free personal accounts on Outlook, Hotmail, Yahoo, iCloud, and AOL almost never accept cold outbound into the inbox folder. The filters are tuned for consumer protection, not professional contact. You can technically send, but the emails go to spam, the mailbox burns, and the recipient never sees the message anyway.

## THE COUNTER-INTUITIVE PROVIDER MATCHING MOVE

When you turn provider matching ON aggressively (Google sends only to Gmail, O365 only to O365), you concentrate sending pressure on a single ESP per domain. **That burns the domain faster on that one ESP.** Try turning provider matching OFF. Distributing the load across recipient ESPs survives longer than forcing a strict 1:1 match. Test against your own data before committing.

## PRINCIPLE 09 · ENTERPRISE ROUTING

## Google Can't Reach Enterprise Gateways.

Google Workspace mailboxes have IP reputations that fail when sending to enterprise security gateways like Barracuda, Mimecast, and Proofpoint. You'll get bounces: not spam-folder placement, actual hard bounces.

## THE DIAGNOSTIC

Filter your leads by **status = bounced**. If Barracuda, Mimecast, Proofpoint, and similar gateways dominate the list, those are all from Google-account sends. SMTP infrastructure with enterprise-grade IP reputation handles those targets without bouncing.

## HOW TO IDENTIFY ENTERPRISE GATEWAYS

Run an MX lookup on the recipient domain. The MX records reveal the gateway:

| MX PATTERN               | GATEWAY         | ROUTING                     |
|--------------------------|-----------------|-----------------------------|
| barracuda.*              | Barracuda       | SMTP infrastructure or O365 |
| mimecast.*               | Mimecast        | SMTP infrastructure or O365 |
| pphosted.*               | Proofpoint      | SMTP infrastructure or O365 |
| mxlogic.*                | McAfee MX Logic | SMTP infrastructure or O365 |
| google.com / outlook.com | Standard ESPs   | Any healthy infrastructure  |

## THE ROUTING RULE

If your ICP includes enterprise companies behind security gateways, **don't send from Google Workspace accounts to them**. Segment your list by MX gateway, route enterprise targets through SMTP infrastructure or O365 mailboxes, and keep Google accounts for SMB and mid-market only.

## PRINCIPLE 10 · THE GMAIL ASYMMETRY

## Personal Gmail Burns 3-5x Faster.

Sending to personal Gmail addresses burns mailboxes 3 to 5x faster than sending to Google Workspace business addresses, even though both are technically "Google."

### REASON 01: DIFFERENT SPAM FILTERS

Personal Gmail and Google Workspace share a parent company but operate completely independent spam filters. You can be fully inboxed on Workspace while fully spamming on personal Gmail, and vice versa. Workspace being healthy doesn't imply Gmail is healthy.

### REASON 02: AGGRESSIVE CONSUMER FILTER

Personal Gmail's filter is built for anti-scam protection, designed to defend everyday consumers. Workspace assumes the recipient is a professional who can handle a cold email; Gmail assumes the recipient is your grandmother.

### REASON 03: ZERO WARM-UP SIGNAL

Sequencers don't include personal Gmail accounts in their warm-up loops by design. Cold outbound is meant to target businesses. So your mailbox accumulates zero warm-up signal against personal Gmail. Every send is cold from the recipient ESP's perspective, no matter how mature the mailbox is.

### CRITICAL IMPLICATION FOR TESTING

Placement tests against Google Workspace seed accounts will tell you **nothing** about how you're landing on personal Gmail. If you're targeting personal recipients, your placement test is essentially blind. The only real signal is reply rate from those recipients.

### THE TAKEAWAY

If you're targeting personal Gmail, expect shorter mailbox lifespans, plan rotation accordingly, and don't trust placement tests as a health signal.

## 11

## PRINCIPLE 11 · REGISTRAR RISK

## Cap At 250 Domains Per Account.

Don't put more than ~250 domains in a single registrar account. If the registrar bans the account (because of a spammy offer or abuse complaint), you lose everything in one move.

**FIELD EVIDENCE**

A client lost ~2,000 domains in a single registrar ban. After that incident, they capped at 250 domains per account before spinning up a new one. No further losses since.

**REGISTRAR CAPABILITIES**

| REGISTRAR                       | API QUALITY | NOTES                                           |
|---------------------------------|-------------|-------------------------------------------------|
| <b>Tier 1: Major Registrars</b> | Excellent   | Bulk operations, easy automation. Cap 250/acct. |
| <b>Tier 2: Bulk-Friendly</b>    | Strong      | Beast-mode bulk naming tools available.         |
| <b>Tier 3: API-First</b>        | Good        | Reliable API, fair pricing.                     |
| <b>Tier 4: Cloud-Native</b>     | Annoying    | Hardest to ban, but harder to automate.         |

**THE BEST PRACTICE**

Multiple accounts **on the same registrar** is often better than spreading across registrars. Example: 4 registrar accounts at 250 each = 1,000 domains, distributed risk, single API integration to maintain. You keep automation simple while still protecting against single-account bans.

**THE MENTAL MODEL**

Think of registrar accounts the way you think of email mailboxes. Each one is a unit of risk. Concentrate too many domains in one account and a single ban event wipes out an entire infrastructure tier.

## PRINCIPLE 12 · NAMING RULES

## No Hyphens. No Numbers.

Domain naming doesn't need an elaborate anti-pattern system, but a few hard rules matter, and getting them wrong groups your entire infrastructure as obvious throwaway sending.

**HARD NO**

- ✗ company-name.com (hyphens)
- ✗ companyone.com / company2.com (numbers)
- ✗ get-yourbrand.com
- ✗ try-yourbrand.com

**ACCEPTABLE**

- ✓ Brandable single-word names
- ✓ Two-word combos without hyphens
- ✓ Regional names
- ✓ Made-up but pronounceable words

## TLD SELECTION

| TLD                 | STATUS | NOTES                                                                             |
|---------------------|--------|-----------------------------------------------------------------------------------|
| .com                | Best   | Default choice. Highest trust.                                                    |
| .co                 | Good   | Strong B2B alternative.                                                           |
| .net                | Good   | Widely accepted. Older trust.                                                     |
| .info               | Okay   | Cheap and acceptable for outbound.                                                |
| .us / country codes | Avoid  | Low trust for outbound.                                                           |
| .io / .ai           | Avoid  | Either expensive or dirt-cheap variants get fingerprinted as spam infrastructure. |

**TOOLING SHORTCUT**

Some registrars offer bulk-domain "beast mode" tools: provide a few keywords plus optional prefixes/suffixes, and the tool generates available variations across acceptable TLDs. This handles naming variation faster than manual selection and avoids the lookalike-domain trap automatically.

## 13

## — PRINCIPLE 13 · IP REPUTATION

## Dedicated IPs Beat Shared Pools.

On shared IPs, your reputation is contaminated by every other sender on that IP. One spammer on the same shared IP and your mailboxes inherit their reputation problems.

**Change nothing in your setup. A neighbor on the IP gets blacklisted. Your reply rates collapse.**

## — THE DIAGNOSTIC SIGNAL

If reply rates drop sharply across **multiple mailboxes simultaneously** with no copy, ICP, or volume changes on your end, suspect IP reputation contamination from a shared neighbor. The simultaneity is the tell. Your changes affect mailboxes one cohort at a time. Shared-IP contamination affects everything riding on that IP at once.

## — WHAT THIS MEANS FOR STACK DESIGN

- For meaningful cold outbound volume, dedicated IPs aren't a luxury. They're table stakes.
- Shared-IP infrastructure (most low-cost mailbox resellers) compounds your risk silently.
- The deliverability "mystery drops" most operators experience are usually shared-IP contamination, not their own mistake.

**THE HIDDEN COST**

Cheap mailbox providers using shared IP pools look 50% cheaper on paper. But when you factor in the time spent diagnosing reputation drops you didn't cause, replacing burned domains, and the lost reply revenue during contamination events, the real cost is multiples higher.

## PRINCIPLE 14 · TRACKING DISCIPLINE

## Stop Tracking Opens.

Open tracking inserts a tracking pixel that ESPs detect and downgrade. Open data has been broken since iOS Mail Privacy Protection rolled out anyway. The data is mostly noise.

**OFF**

- ✗ Open tracking pixel
- ✗ Click tracking redirects
- ✗ Reading-time analytics
- ✗ Anything inserted invisibly into the email body

**MEASURE INSTEAD**

- ✓ Reply rate by mailbox cohort
- ✓ Reply rate by ICP segment
- ✓ Meetings booked / qualified
- ✓ Bounce rate by recipient ESP

## WHY CLICK TRACKING IS EVEN WORSE

Click tracking requires redirects (see Principle 07). The mechanism that captures the click is the same mechanism that gets your domain blacklisted at scale. **Click tracking and deliverability are mutually exclusive** at any meaningful volume.

**THE REAL KPI**

A reply means the email reached the inbox **and** resonated with the recipient. That's the only metric that combines deliverability and conversion in one signal. Optimize for replies. Everything else is vanity.

## THE MPP PROBLEM

Apple Mail Privacy Protection automatically opens every email and downloads tracking pixels, regardless of whether the recipient ever read the message. This means every email you send to an iOS user shows as "opened." The data is structurally broken. There's nothing left to optimize against.

## — PRINCIPLE 15 · SUBJECT LINE FORMULA

## 20+ Subject Lines. All Lowercase.

Subject lines are the single most fingerprintable part of your email because they're the shortest. One subject line across 10,000 sends is a death sentence.

## — THE FORMULA

- **All lowercase.** Matches how humans actually write quick emails.
- **Maximum two words.** Anything longer reads like marketing copy.
- **No spam trigger words.** Free, guarantee, urgent, opportunity, click, win: all out.
- **Pool of 20+ variations.** Apply spintax on top of each variation for compounding diversity.
- **Use company name as a variable** when natural. {{company\_name}} question, re: {{company\_name}}

## THE CLAUDE PROMPT

"Please create 20 different variations of subject lines for this copy. All lowercase, no spam words, maximum two words total. You can use company name as a variable. Output as a plain list, one per line."

## — WHY THE SUBJECT LINE MATTERS MOST

The body of your email is hundreds of words. Variation is mathematically easier. The subject line is two words. There are only so many natural-sounding two-word combinations in any language. **This is the bottleneck of variation**, and the easiest place for filters to fingerprint your operation.

## COMPOUNDING VARIATION

20 base subject lines x spintax on each x company name variables = thousands of unique surface-level signatures, even though the underlying intent is the same. This is what survives ESP clustering algorithms.

## — PRINCIPLE 16 · LIST HYGIENE

## Maintain A Global **Suppression List**.

Maintain a global suppression list of mailboxes that have bounced, complained, unsubscribed, or proven dead in past campaigns. Apply across all future campaigns.

## — WHAT TO SUPPRESS

- **Hard bounces.** The address doesn't exist. Sending again does nothing but burn IP reputation.
- **Bounces in the past 90 days.** The address may be valid now, but ESPs remember the bounce history and will downgrade you for retrying too soon.
- **Unsubscribe requests.** RFC 8058 one-click unsubscribe is now table stakes for cold outbound. Honor every request.
- **Spam complaint addresses.** Anyone who marked your previous email as spam.
- **Catch-all addresses that never engage.** They count as sends but never produce replies. Pure mailbox burn.

## — THE COMPOUNDING BENEFIT

The suppression list grows over time. Every campaign you run feeds the list. Every future campaign benefits from the cleanup of every past campaign. **This is the only deliverability lever that gets stronger the longer you operate.**

**THE MENTAL MODEL**

Think of the suppression list as institutional memory. Without it, every campaign re-discovers the same dead addresses and re-burns the same mailboxes. With it, your infrastructure compounds in efficiency over time.

## — IMPLEMENTATION DISCIPLINE

Most sequencers have native suppression. Use it globally, not per-campaign. Cross-campaign suppression is what compounds. If you can, also suppress at the **mailbox infrastructure level** so even campaigns set up by other team members inherit the protection automatically.

## — PRINCIPLE 17 · VALIDATION PROTOCOL

## Placement Test **Before** Scaling.

Before you ramp a sequence to full volume, send a placement test. If it lands in spam on Google Workspace or Microsoft, fix it before you burn through any volume.

## — THE LIGHTWEIGHT TEST (NO TOOLS)

- 01 Duplicate your sequence in the sequencer.
- 02 Set the recipient to your own seed inbox: one Google Workspace + one Microsoft.
- 03 Send one email per mailbox provider you intend to scale.
- 04 Manually check inbox vs. spam placement on each.
- 05 If anything hits spam, diagnose before you scale a single additional send.

## — THE HEAVIER TEST (MANAGED SEED NETWORK)

- Use a managed placement testing service to test against a network with real ESP accounts.
- **Important:** delete the Outlook, Yahoo, and free Hotmail seeds from your test set if you're not targeting those. They inflate volume to ESPs you don't care about and skew the report.
- Run placement tests **per domain**, not per mailbox. One mailbox test reveals the domain status (see Principle 06).

**CRITICAL CAVEAT**

Placement tests are a decent signal for whether a domain is burned against Google Workspace and Microsoft. They tell you nothing about deliverability to personal Gmail addresses, because seed networks don't run personal Gmail seeds. If your campaign targets personal Gmail, treat placement tests as one signal among many, not the source of truth.

**Test the seed inbox **before** you spend on the full list. The diagnostic is free.**

## — PRINCIPLE 18 · EARLY WARNING SYSTEM

## The Pre-Burn Diagnostic Window.

Reply rate degradation is your earliest warning signal. If you catch it when reply rate first dips, you can save the mailboxes by switching copy. If you wait until they're in spam, the mailboxes are dead.

## — THE WINDOW IN PRACTICE

Catching the issue early means swapping copy fixes the problem and the mailbox returns to inbox placement. Wait too long, and the mailbox is so contaminated that no copy change saves it. Once burned, it has to be replaced, and the replacement cost compounds across your domain pool.

## — THE MONITORING THRESHOLD

- Track reply rate **weekly** per mailbox cohort.
- If reply rate drops by **>25%** week-over-week with the same ICP and copy, **pause and rotate copy immediately**.
- Don't wait to confirm "trend." By the time the trend is confirmed, the mailboxes are gone.

**THE OPERATOR'S DILEMMA**

Most operators are biased toward "wait and see." They want one more week of data to confirm the dip is real. **That extra week is exactly what kills the mailbox.** When in doubt, swap copy. The downside of swapping unnecessarily is small. The downside of waiting too long is total mailbox loss.

## — TOOLS THAT HELP

- **Third-party analytics tools** that aggregate reply rate by ESP and recipient type, surfacing underperforming mailboxes and domains automatically.
- **Custom dashboards** built on top of sequencer APIs: the more granular your view (per cohort, per domain, per ICP segment), the earlier you'll catch the drop.

## PRINCIPLE 19 · WARM-UP DISCIPLINE

# Warm-Up Is Preventative, Not Curative.

Warm-up only works for brand new mailboxes before first send, or for mailboxes between campaign rotations as a cooling-off period. It cannot rescue what's already burned.

## WHAT WARM-UP CANNOT DO

- Rescue a mailbox that's already in spam.
- Substitute for actual engagement on real campaigns.
- Improve a domain's reputation faster than 2 to 3 weeks.

## THE WARM-UP TIMELINE

## DAYS 1-14

Pure warm-up only. Zero campaign volume. Building baseline reputation across recipient ESPs.

## DAYS 15-21

Light campaign volume (10 to 20 emails/day) alongside continued warm-up. Test placement before ramping further.

## DAY 22+

Mailboxes ramp to full outbound capacity. Warm-up continues alongside campaigns at a 1:1 ratio between outbound sends and warm-up sends.

## THE 1:1 RULE

Every campaign email gets matched by a warm-up email. Maintain this ratio for the entire active life of the mailbox, not just the early weeks. Warm-up is not a phase that ends. It runs continuously alongside campaigns, providing the engagement signal that keeps the mailbox in the inbox.

## THE PROVIDER OVERRIDE

If your warm-up provider specifies a different ratio for their tool, follow theirs. The 1:1 rule is the safe default, but providers tuning their network may have data on better ratios for their specific seed list. Always defer to provider guidance over generic rules.

## PRINCIPLE 20 · WHEN THINGS GO WRONG

## Don't Rotate Infrastructure With Burned Copy.

When mailboxes burn, the instinct is to provision new infrastructure and keep moving. Wrong move. If you swap the infrastructure but keep sending the same copy that burned the previous batch, the new mailboxes inherit the same fate, in days, not weeks.

**New mailboxes + burned copy = new zombies.**

## WHY IT HAPPENS

The same fingerprinting logic from Principle 06 applies to copy. ESPs cluster sending patterns by structural signature, not by domain. When the previous batch burned because of copy, that copy structure is already flagged at the ESP level. New domains don't reset the clock on burned copy. They ride into the spam folder with the fingerprint.

## THE FIX: IN ORDER

- 01** Diagnose copy first. Before you spend a dollar on new infrastructure, confirm whether copy is the variable that broke. If reply rate dropped while ICP, volume, and infrastructure stayed identical, copy is the cause.
- 02** Build new copy before new mailboxes. Generate 5+ structurally different variants (Principle 02). Test placement on the existing infrastructure. If the existing infra is too far gone to test cleanly, build copy first anyway. It's cheap insurance.
- 03** Provision new infrastructure with new copy locked in. The new batch ships day-one with the new copy. The burned copy never touches the new mailboxes.
- 04** Keep the new copy in rotation across cohorts going forward. See Principle 01: copy fatigue is a continuous problem, not a one-time fix.

## THE RULE THAT SAVES YOU

Make it a default operating practice: every new batch of mailboxes ships with structurally different copy from the previous batch. Even if the previous batch was healthy. Even if reply rates were great. By the time you're rotating mailboxes, the copy is already old enough to be at risk on the next cohort.

## ACTION SHEET · THE 15-STEP FIRE DRILL

# Quick-Reference Action Sheet.

The condensed playbook for any new client or any deliverability fire drill. Run this sequence in order. The earlier steps unlock the later ones.

- |                                                                                                                       |                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>01</b> <b>Audit copy variation.</b> 5+ structural variants. Spintax on each. 20+ subject pool.                     | <b>02</b> <b>Audit sender names.</b> One unique name per mailbox. No hyperlinked company names.          |
| <b>03</b> <b>Kill all redirects</b> if sending >10k/day. Domain masking, then no domain.                              | <b>04</b> <b>Clean Google Maps lists.</b> Strip Outlook, Hotmail, Yahoo, iCloud, AOL personal addresses. |
| <b>05</b> <b>Audit provider matching.</b> Try OFF. Measure mailbox longevity.                                         | <b>06</b> <b>Audit enterprise routing.</b> Barracuda/Mimecast/Proofpoint targets via SMTP or O365 only.  |
| <b>07</b> <b>Set rotation cadence.</b> 3 weeks active, then warm-up, then fresh batch. 3x peak infrastructure.        | <b>08</b> <b>Enable suppression list.</b> Bounces, complaints, unsubs, dead catch-alls.                  |
| <b>09</b> <b>Diversify domains.</b> 250 max per registrar account. No hyphens. No numbers. .com / .co / .net / .info. | <b>10</b> <b>Disable open tracking.</b> Click tracking off too.                                          |
| <b>11</b> <b>Placement test before scaling.</b> Managed seed network + manual seed check. Blind for personal Gmail.   | <b>12</b> <b>Monitor reply rate weekly.</b> >25% drop = rotate copy immediately.                         |
| <b>13</b> <b>Kill burned mailboxes fast.</b> Cancel subscription first, then delete. Replace from warm-up pool.       | <b>14</b> <b>Maintain 1:1 warm-up ratio</b> for the active life of every mailbox.                        |
| <b>15</b> <b>Reset both clocks together.</b> New infrastructure ships with structurally new copy. Always.             |                                                                                                          |