

THE MOONGIE PLAYBOOK

Cold Email System

The complete B2B outbound guide - from ICP to inbox placement. Infrastructure, list hygiene, messaging, cadence and monitoring in one place.

98.7%

INBOX PLACEMENT

~4.5%

REPLY RATE

~0.8%

BOUNCE RATE

1,500+

MAILBOXES MANAGED

Why deliverability comes first

The best cold email ever written is worthless in spam. Before copy, before targeting, before tooling, your message has to physically arrive in the primary inbox - and that is decided by infrastructure, reputation and habits, not luck.

Most teams do it backwards. They rewrite subject lines forever and never check whether they are landing in the inbox. They obsess over copy and ignore authentication. They send from their main domain and wonder why invoices start going to junk.

This playbook fixes that. It collects everything we apply to every campaign at Moongie: the strategy, the infrastructure, the list hygiene, the messaging, and the monitoring. None of it is a hack. All of it compounds. Skip one layer and the others work less. Apply all of it and cold email becomes a quiet, predictable pipeline channel.

Four parts. Five metrics to watch. One master checklist at the end. Steal everything.

What's inside

PART	WHAT YOU'LL FIND
1 · Strategy	ICP definition · Shared vs. dedicated infrastructure
2 · Infrastructure	Lookalike domains · SPF / DKIM / DMARC · Warmup · Volume discipline
3 · List & Data	Bounce rate · Catch-all emails · Google & Yahoo compliance
4 · Campaign	First email structure · Email + LinkedIn cadence · Follow-ups
5 · Monitoring	Inbox placement testing · Reply rate benchmarks · Blacklists · Hygiene

PART 1 OF 5

Strategy Foundation

Before a single domain is registered, two questions decide everything: who are you emailing, and what infrastructure will carry it?

CH. 01 **Build a tight ICP** - make cold email feel warm

CH. 02 **Choose your infrastructure** - shared vs. dedicated

Build a tight ICP - make cold email feel warm

Cold email gets a bad reputation because most of it is sent to the wrong people. The fix is not better copy or a clever subject line. It is a sharper Ideal Customer Profile.

What an ICP actually is

An ICP is a precise description of the company and person most likely to buy from you, stay, and refer others. It covers firmographics (industry, size, geography), the buyer's role, and the specific problem you solve.

The mistake most teams make: confusing an ICP with a target market. A target market is "B2B logistics software." An ICP is "operations leads at 50-200 person freight brokerages in the US who still run dispatch on spreadsheets." One you can write a relevant email to. The other you cannot.

A cold email feels warm the moment the reader thinks "this is about me" instead of "this is about them."

How to build your B2B ICP - in order

1. **Firmographics:** industry, company size, geography, business model. Be concrete - "20-200 employees" beats "SMB."
2. **The trigger:** what recent event makes this problem urgent? New funding, a hire, a tool migration, a regulation, a growth spurt. Triggers turn cold leads warm.
3. **The role and the pain:** the exact title that owns the problem, plus the words they use to describe it - their jargon, not yours.
4. **The buying context:** who signs off, what they currently use instead, what "good enough" looks like today.
5. **Disqualifiers:** who looks like a fit on paper but never buys. Naming these saves more time than any positive criterion.

How narrow?

Narrow enough that you can name the trigger and write a line no competitor could copy-paste. A list of 500 perfectly matched prospects with a relevant message will out-reply 5,000 vague ones - and protect your domain reputation while doing it.

ICP → Copy

The trigger becomes your opening line. The pain becomes your value statement. The buying context shapes your CTA: "worth a 15-minute look?" vs. a direct demo booking link.

ICP setup checklist

- ☐ Defined by firmographic AND trigger, not just industry
- ☐ Can be written in one readable paragraph (not a slide deck)
- ☐ Names specific disqualifiers
- ☐ Maps to the exact role that owns the problem
- ☐ Informs your first line of copy directly
- ☐ Tested against real reply data and refined by segment

Choose your infrastructure - shared vs. dedicated

Most people pick based on price without understanding what they are buying. This chapter explains the real trade-offs.

SHARED INFRASTRUCTURE

What it is: multiple senders use overlapping sending resources - often shared IPs.

Good for: testing outbound, small lists, fast on-ramp, lower cost.

Risk: one sender blasting a dirty list can drag the whole pool's reputation down - through no fault of yours.

DEDICATED INFRASTRUCTURE

What it is: the IPs, domains and mailboxes belong to you and only you.

Good for: sustained volume, long-term brand asset, clean attribution when diagnosing issues.

Risk: you own the downside - no pool to dilute list or copy mistakes.

Shared infrastructure is fine until your reputation depends on a sender you will never meet.

The thing most debates miss

The model matters less than the operations around it. A dedicated setup with no monitoring will land in spam just as reliably as a toxic shared pool. The real question is: **who is watching deliverability every single day?**

Decision checklist

- ☐ **Volume:** low and exploratory → shared; sustained and growing → dedicated
- ☐ **Time horizon:** months and beyond favours dedicated (reputation compounds)
- ☐ **Tolerance for others' mistakes:** none → dedicated
- ☐ **Warmup window:** have 3-4 weeks? Dedicated is on the table
- ☐ **Daily monitoring:** if nobody is watching, neither model is safe
- ☐ **Channel importance:** core to pipeline → owned, dedicated infrastructure

PART 2 OF 5

Infrastructure Setup

Get the foundation wrong and nothing downstream matters. This is the part most teams skip and then blame the channel.

CH. 03 **Lookalike sending domains** - protect what you cannot replace

CH. 04 **Authentication** - SPF, DKIM, DMARC

CH. 05 **Warmup** - the 3-4 weeks you cannot skip

CH. 06 **Volume discipline** - 25 per mailbox, scale with more

Lookalike sending domains - protect what you cannot replace

Your primary domain is the one asset you cannot replace. Cold email can damage its reputation in ways that are slow and expensive to undo.

Your main domain is for the business you have. Lookalike domains are for the business you are trying to win.

What a lookalike domain is

A lookalike sending domain closely resembles your main brand domain but is registered specifically to send cold email. If your company is at `acme.com`, a lookalike might be `acme-hq.com`, `getacme.com`, or `tryacme.com`. These carry their own reputation and authentication records. If one degrades, you rotate it out - your brand domain stays untouched forever.

How to pick good lookalike domains

- **Stay recognizable.** Use `get`, `try`, `go`, or `-hq` variants. `getacme.com` reads as Acme. `acme-marketing-team-2026.com` reads as spam.
- **Prefer common TLDs.** `.com` first, then `.co` or `.io`. Avoid cheap, abuse-heavy TLDs that filters distrust.
- **Check the history.** A previously owned domain may carry blacklist baggage. Buy fresh when unsure.
- **Avoid character tricks.** No swapping letters for numbers. That is what phishers do.
- **Buy domains you would happily put on a landing page.** Because you should - a domain that loads nothing looks abandoned.

Standard starting setup

3 sending domains × 3 mailboxes each = 9 senders = ~225 emails/day = ~4,500/month at safe volume. Need more? Add another set of domains - never raise the per-mailbox cap.

Domain setup checklist

- ☐ Lookalike domains registered (primary domain never touches cold email)
- ☐ Domains point to a real landing page, not a blank page

☐ SPF, DKIM, DMARC configured on every domain

☐ History checked - no prior blacklist baggage

☐ Custom tracking domain set up (links carry your reputation, not a shared one)

☐ Warmed before any real sends

Authentication - SPF, DKIM, DMARC

If your cold emails are landing in spam, the first thing to check is not your copy. It is your authentication. Since 2024, Gmail and Yahoo require all three on every sending domain.

If SPF, DKIM, and DMARC are not set, you are not doing cold email - you are doing cold guessing.

SPF - who is allowed to send

A single TXT record listing the servers allowed to send mail for your domain.

```
v=spf1 include:_spf.google.com ~all
```

One record only. Under 10 DNS lookup limit. Combines all includes into one line.

DKIM - the cryptographic signature

Your platform holds a private key; you publish the public key in DNS. Survives forwarding. Non-negotiable for outbound.

After setup: send yourself a test and confirm `dkim=pass` in the headers.

DMARC - the policy

Start at `p=none` (monitoring mode), watch the reports, then tighten.

```
v=DMARC1; p=none;
rua=mailto:dmarc@yourdomain.com
```

After clean reports: move to `p=quarantine`, then `p=reject`.

Critical: DMARC alignment

DMARC passes when the From domain matches the domain validated by SPF or DKIM. SPF and DKIM can both pass while DMARC fails - check alignment explicitly.

Authentication setup checklist

- ☐ One SPF TXT record, under 10-lookup limit, ending in `~all`
- ☐ DKIM enabled in platform AND public key live in DNS
- ☐ Test email shows `spf=pass` and `dkim=pass` in headers
- ☐ DMARC record at `p=none` with working `rua=` address

☐ DMARC alignment confirmed (From domain matches SPF or DKIM domain)

☐ Sending domain separate from primary business domain

☐ Records verified after DNS propagation (not immediately after pasting)

☐ Custom tracking domain set up

Moongie tip: Authentication is a 30-minute job that prevents months of mysterious spam-folder pain. We re-verify ours automatically on every domain, every day.

Warmup - the 3-4 weeks you cannot skip

A fresh domain is a blank slate. To Google, Microsoft, and Yahoo, it could just as easily belong to a spammer as a real business. Warmup fills that slate with positive signals.

Warmup is not the cost of doing cold email. It is the deposit that makes everything after it work.

What actually happens, week by week

WEEK	WHAT'S HAPPENING	VOLUME
Week 1	Tiny volume, high engagement. Every email opened and replied to. Messages that slip to spam get rescued - a powerful "wanted mail" signal.	5-10/day
Week 2	Volume increases steadily. Provider starts seeing a consistent daily rhythm. Engagement stays high.	10-20/day
Week 3	Approaching real volume. Reputation established enough that messages reliably land in primary inbox.	15-25/day
Week 4	Volume holds steady. Deliverability monitored. Mailbox confirmed placing reliably before a single prospect is touched.	25/day

What breaks when you rush it

A rushed warmup fails silently: open rates look "a bit low," replies dry up, then a placement test shows 80% in spam. By that point the damage is done and often the only fix is new domains and another full warmup - you lose more weeks than you ever "saved."

If a vendor promises full volume in week one, they are burning your domains. Walk away.

Pre-warmup checklist

- ☐ Domains registered
- ☐ SPF, DKIM and DMARC configured and verified on every sending domain
- ☐ Custom tracking domain set up

□ Clean, verified list waiting (warmup protects mailbox; a dirty list still spikes bounces)

□ Copy that reads like a human wrote it to one person

□ Clear plan for follow-up and channel mix

Volume discipline - 25 per mailbox, scale with more

Inbox providers do not just count how much you send - they count how much each mailbox sends. One account blasting 200 emails a day pattern-matches to a spammer. Nine accounts sending 25 each look like a normal sales team on a normal Tuesday.

Volume discipline is invisible when it works and catastrophic when it's missing. It is the cheapest insurance in cold email.

The math at different volumes

MAILBOXES	EMAILS / DAY	EMAILS / MONTH (~20 DAYS)
9 (3 domains × 3)	225	~4,500
18 (6 domains × 3)	450	~9,000
30 (10 domains × 3)	750	~15,000
75 (25 domains × 3)	1,875	~37,500

How to scale without breaking the rule

Need more volume? You do not raise the cap. You add more domains and mailboxes, warm them for 3-4 weeks, and plug them into the rotation. Each increment is safe, monitored and reversible.

Nobody, ever, raises a mailbox past its cap. The setup grows by adding more warmed mailboxes - never by pushing existing ones harder.

PART 3 OF 5

List & Data

The best infrastructure in the world cannot save you from a dirty list.
Data quality is a deliverability decision.

CH. 07 **List verification and bounce rate**

CH. 08 **Catch-all emails** - send, skip or verify?

CH. 09 **Google and Yahoo bulk sender compliance**

List verification and bounce rate

Every bounce is a message to inbox providers, and a high bounce rate tells them you do not know who you are emailing. That signal follows you for weeks.

1% BOUNCE TARGET (MAX)	0.8% MOONGIE LIVE AVERAGE	2-3% PROVIDERS GET SUSPICIOUS	5%+ SERIOUS REPUTATION DAMAGE
-------------------------------------	--	--	--

A bounce is not a wasted email. It is a vote cast against your reputation, counted for weeks.

What causes a high bounce rate

- **Stale or scraped data.** People change jobs constantly. A list accurate six months ago is full of dead B2B addresses today.
- **Catch-all and role addresses.** Generic inboxes like info@ or sales@ are unpredictable and often bounce.
- **No authentication.** Without SPF/DKIM/DMARC, some servers reject your mail outright - a bounce and a reputation hit simultaneously.
- **Cold domains sending too fast.** A brand-new domain blasting hundreds of emails on day one looks exactly like a spammer.

Verification process - in order

- ☐ Syntax & domain checks first - cheap and instant
- ☐ SMTP verification second - confirms the mailbox exists
- ☐ Catch-all risk scoring third - see Chapter 08 for the decision tree
- ☐ Remove role accounts: info@, office@, sales@, admin@, noreply@
- ☐ Re-verify any segment older than 3 months before reuse
- ☐ Monitor bounces daily and pause any mailbox or domain that spikes

Moongie tip: A smaller clean list beats a big dirty one every single time. We cut anything questionable and never regret it.

Catch-all emails - send, skip or verify?

A catch-all domain accepts mail sent to any address - even ones that don't exist. Your verifier marks these as "unknown." That label is not a failure; it is the tool being truthful about uncertainty.

A catch-all result is not a green light or a red light. It is the server refusing to answer, and you have to decide how much that silence is worth.

The decision tree - stop at the first rule that applies

#	CONDITION	ACTION
1	Person verified elsewhere (LinkedIn, company page, press mention)	Send
2	Email pattern confirmed from another verified address at the same domain	Send
3	Generic or guessed address: info@, sales@, contact@ with no human confirmation	Skip
4	Important target, no pattern confirmed yet	Verify deeper
5	Domain reputation still fragile (new or recently warmed)	Skip low-confidence

How to verify a catch-all more deeply

- Confirm the human exists - LinkedIn profile, conference speaker bio, author byline, team page
- Lock the email pattern from one fully verified address at the same domain
- Use multi-signal verifiers (SMTP probing + historical engagement data + pattern databases)
- Watch role-based prefixes: `admin@`, `noreply@`, `webmaster@` - rarely your buyer
- Test high-confidence catch-alls in small batches first and watch the bounce response

Google & Yahoo bulk sender compliance

Since early 2024, Gmail and Yahoo enforce a shared set of sender standards - and they do not care whether you call your messages "marketing," "transactional," or "cold outbound."

If a rule only kicks in "at volume," assume the filter is already grading you on it today.

The three requirements - all mandatory

1. AUTHENTICATION

SPF, DKIM, and DMARC on every sending domain. DMARC alignment required (From domain matches what SPF or DKIM authenticate).

2. ONE-CLICK UNSUBSCRIBE

A working `List-Unsubscribe` header that honors opt-outs. This is good practice anyway - every cold sequence should include a no-friction opt-out.

3. LOW SPAM COMPLAINT RATE

Keep it consistently low. Spikes are treated as a red flag. People who get irrelevant messages do not unsubscribe - they report you.

4. BOUNCE RATE

Under 1% target. High bounce rates are themselves a reputation signal that both providers watch closely. Clean lists, always.

Compliance checklist

- ☐ SPF, DKIM, DMARC correctly configured on every sending domain
- ☐ DMARC alignment verified (From domain matches SPF or DKIM domain)
- ☐ One-click unsubscribe header in every sequence
- ☐ Spam complaint rate monitored and consistently low
- ☐ Bounce rate under 1%
- ☐ Per-mailbox volume capped (~25/day)
- ☐ Sequences stop automatically on any reply

PART 4 OF 5

Campaign Execution

The infrastructure is ready. Now you earn the reply.

CH. 10 **Write to one reader**, about their problem

CH. 11 **The email + LinkedIn cadence** - familiarity multiplies replies

CH. 12 **Follow-ups and the break-up email**

Write to one reader, about their problem

Cold email dies when it reads like a campaign. Write as if to one specific person, about one specific problem, in under 90 words.

What a good first email looks like

- **Under 90 words.** Brevity proves respect.
- **No links, no attachments.** They trigger filters. Earn the right to share a link in reply.
- **One idea, one soft question.** Not "Can we book 30 minutes?" - "Worth a quick look?"
- **Subject lines: 2-4 plain words, lowercase, zero clickbait.** A subject line is a promise, not a headline.
- **Personalization that proves research** - not just a {first_name} token.

First email structure

1. **Opening line:** their situation, a trigger event, or a problem they'd recognize. Written about them, not you.
2. **Value statement:** one sentence on what you help people like them do - in their language.
3. **Social proof** (optional): one relevant result, stated plainly.
4. **Ask:** a single, low-friction question. Make the bar to reply as low as possible.

Would a busy stranger thank you for this email? If not, rewrite it.

Subject lines that work vs. don't

WORKS	DOESN'T WORK
dispatch software	Revolutionize Your Operations in 2026!
quick question	Following up on my previous email
freight reconciliation	Hope this finds you well 😊
saw your job post	FREE STRATEGY CALL - Limited Spots!

The email + LinkedIn cadence - familiarity multiplies replies

When a prospect has seen your face on LinkedIn before your email arrives, you stop being a stranger. In our campaigns, coordinated email + LinkedIn cadences consistently multiply reply rates versus a single channel.

The cadence, day by day

DAY	CHANNEL	ACTION
Day 1	Email	Email #1: under 90 words, one idea, one soft question. No links. Plain text.
Day 3	LinkedIn	Profile view + connection request. Short personal note on the same theme. Never "I sent you an email."
Day 6	Email	Email #2: a new angle. An insight, a benchmark, a relevant example. Still short.
Day 10	LinkedIn	DM for accepted connections. Casual and human - this is where many of the best conversations start.
Day 15	Email	Email #3: the graceful break-up. Routinely the highest-reply step of the entire sequence.

By touch three you are not a stranger anymore. That is the entire trick.

The three rules that keep it working

1. **Every touch knows about every other touch.** The moment someone replies anywhere - email, DM, even a comment - the rest of the sequence stops. Nothing torches goodwill like a follow-up after an answer.
2. **Human-like limits on LinkedIn.** Gradual ramp-up, conservative daily caps, personalized notes. Account safety beats one extra touch, always.
3. **Channels carry different jobs.** Email does the reasoning; LinkedIn does the familiarity. Do not copy-paste the same message into both.

Starting sequence: build the email foundation first (3-4 weeks of warmup). Once the email engine is running clean and you can see real inbox placement numbers, add LinkedIn as a multiplier - not a distraction.

Follow-ups and the break-up email

Most replies come from follow-ups, not openers. But each follow-up must add something new - never "just bumping this."

What makes a good follow-up

- Adds a new angle, not a repetition of the first email
- References the previous touch without making it awkward
- Stays short
- One new idea, one new question

Good follow-up angles

- A relevant benchmark or data point
- A similar client result
- A new reason why now (trigger event)
- A challenge or reframe of the status quo

The break-up email

The graceful break-up is routinely the highest-reply email in the entire sequence. Why?

Because it is the only touch that is genuinely human - it acknowledges the silence, removes pressure, and leaves the door open.

Structure

1. Acknowledge you have reached out a few times
2. State simply that you will not follow up again
3. Leave one last clear reason to reply
4. Make the ask as easy as possible

Stop the sequence the instant someone replies anywhere. Nothing torches goodwill like a follow-up after an answer.

Sequence length: the sweet spot

3-4 emails over 2-3 weeks. Enough time for different circumstances to intercept (timing matters more than copy), enough touches to establish familiarity, and a graceful exit that does not feel like harassment.

PART 5 OF 5

Monitoring & Optimization

The campaign is running. Now you protect it.

CH. 13 **Inbox placement testing** - "delivered" is not "inbox"

CH. 14 **Reply rate benchmarks** - what good actually looks like

CH. 15 **Blacklist monitoring and recovery**

CH. 16 **Ongoing hygiene** - suppression, pruning, rotation

Inbox placement testing - "delivered" is not "inbox"

Your sending tool says 497 emails were "delivered." That number tells you almost nothing about whether anyone saw them. "Delivered" means the receiving server accepted the message - which includes accepting it straight into spam.

"Delivered" is the email industry's most expensive lie - it tells you the door opened, not that anyone walked through.

What good placement looks like

INBOX %	STATUS	ACTION
95%+	Healthy	Ship it and monitor weekly
80-95%	Functional but leaking	Find what's dragging - warmup, content or auth
Below 80%	Stop and fix	Every additional send teaches providers you belong in spam
Promotions	Not ideal for 1-to-1	Tighten copy - reads like marketing, not a colleague

98.7%

MOONGIE INBOX PLACEMENT

Daily

TESTING FREQUENCY

1,500+

MAILBOXES MONITORED

What makes placement drop (in order of frequency)

1. **Authentication gaps.** Missing or misaligned SPF/DKIM/DMARC.
2. **Volume that outruns reputation.** New domains cannot send like aged ones.
3. **Rushed or skipped warmup.** A domain with no trust is treated like a stranger.
4. **Bounces from bad data.** High bounce rates signal "scraped list" to spam filters.
5. **Content and links.** Tracking links on shared domains, link shorteners, image-heavy templates.

Testing cadence

- Before every new campaign launch
- Weekly while the campaign is running

- Immediately after any change (new domain, new copy, volume increase, reply-rate drop)

Reply rate benchmarks - what good actually looks like

You sent 500 cold emails and got 12 replies. Is that good? Most benchmark articles quote different numbers with no context. Here are honest ranges.

Honest expectations by scenario

SCENARIO	REPLY RATE	WHAT IT MEANS
Broad list, generic offer	Under 1%	You are spraying. Expect spam complaints, not replies.
Decent ICP, average copy	1-3%	This is where most senders live.
Tight ICP, relevant offer, good deliverability	3-5%	This is "good."
Narrow niche, strong proof, personalised angle	5%+	Usually smaller, smarter sends.

Total reply rate is vanity. Positive reply rate is the metric that books meetings.

The metric that actually matters

Track both total reply rate and positive reply rate. The gap between them tells you whether your problem is volume or message-market fit:

- **Low total reply rate, clean deliverability** → targeting or offer problem
- **Healthy total reply rate, low positive rate** → wrong audience or misleading hook
- **Good positive rate, few meetings** → your booking step or landing page is the leak

How to improve reply rate - in order

1. Confirm inbox placement (test before scaling)
2. Lock down authentication
3. Use lookalike domains, not your primary
4. Verify and clean your list (bounce rate under 1%)
5. Tighten your ICP
6. Lead with one relevant reason (one "why you, why now")

7. Send follow-ups (most replies come from message 2 or 3)

8. Add LinkedIn as a second channel

Blacklist monitoring and recovery

Replies dried up overnight. Bounces spiked. Before you panic, you need facts: is your domain or sending IP actually listed, where, and why.

How to run a blacklist check - in order

1. Find your real sending IP (open raw email headers, look for the `Received` line closest to your sending server)
2. Check the IP against an aggregated DNSBL lookup (MXToolbox, MultiRBL, Spamhaus)
3. Check your root domain and any link domains separately
4. Confirm against the specific blacklists directly (aggregators sometimes lag)
5. Run an inbox placement test regardless - catches invisible provider-level filtering no public check shows

Why you ended up on a blacklist

None of these are bad luck - they are sending decisions:

- **Bad lists.** Scraped or unverified addresses produce hard bounces and spam-trap hits.
- **No or broken authentication.** Missing SPF, DKIM, or DMARC.
- **Volume that spikes from zero.** A new domain blasting hundreds of emails on day one.
- **Skipped or rushed warmup.**
- **Complaints.** Irrelevant outreach to the wrong people.

How to get delisted - step by step

1. **Stop sending immediately** from the affected domain or IP
2. **Diagnose and fix the root cause** - delist without fixing this and you will be back
3. **Find the delisting page** for each list that flagged you (Spamhaus, Barracuda - most have self-service forms)
4. **Submit honestly.** Describe what went wrong and what you changed.
5. **Wait and re-check.** Some lists clear in hours, others in a few days.
6. **Rebuild reputation slowly.** Treat a delisted domain like a new one - full warmup.

Ongoing hygiene - suppression, pruning, rotation

Reputation is a balance you either grow or spend. Protecting it requires boring, consistent hygiene - not one-time setup.

The three ongoing disciplines

SUPPRESSION

Customers and past prospects should **never receive cold email**. Build and maintain a suppression list. Every satisfied customer who gets cold-outreached is a brand hit and a potential complaint.

BOUNCE PRUNING

After every send, remove hard bounces immediately. Do not let stale addresses accumulate. Re-verify any segment older than 3 months before sending again.

DOMAIN ROTATION

When metrics on a domain start drifting - lower inbox placement, slightly elevated bounces - **rest the domain before it is burned**. Warmed spares make this painless.

DAILY MONITORING

Someone watching the gauges every day so problems get caught at 92% placement, not discovered at 60%. This is what "managed infrastructure" actually means.

The weekly monitoring ritual

- ☐ Check inbox placement across all active domains (target: 95%+)
- ☐ Check blacklists for all sending IPs and domains
- ☐ Review bounce and complaint rates by domain
- ☐ Prune any addresses that bounced
- ☐ Flag any domain that has drifted below 90% placement for review
- ☐ Confirm warmup is on schedule for any new domains in the pipeline
- ☐ Update suppression list after any reply or opt-out

Deliverability is not a setting you toggle. It is a set of habits - and the habits compound.

Everything on one page

STRATEGY - BEFORE ANYTHING

- ☐ ICP defined: firmographic + trigger + role (one readable paragraph)
- ☐ Disqualifiers named
- ☐ Infrastructure model chosen (shared or dedicated)
- ☐ Target list researched against ICP definition

DOMAIN SETUP

- ☐ Lookalike domains registered (primary domain untouched)
- ☐ Domains point to a real landing page
- ☐ SPF: one record, under 10-lookup limit, ending in ~all
- ☐ DKIM: platform enabled + public key live in DNS
- ☐ DMARC: p=none with working rua= address
- ☐ DMARC alignment verified
- ☐ Custom tracking domain set up
- ☐ Domain history checked (no prior blacklist baggage)

WARMUP

- ☐ 3-4 week warmup scheduled (never shorter, never skipped)
- ☐ Warmup sequences switched on from day one
- ☐ Per-mailbox volume cap hard-set at 25/day
- ☐ Placement monitored throughout warmup period

CAMPAIGN COPY

- ☐ Email #1 is under 90 words
- ☐ Email #1 has no links and no attachments
- ☐ Subject line: 2-4 plain words, lowercase
- ☐ Opening line is about the reader's situation, not your company
- ☐ One idea, one soft question as CTA
- ☐ Follow-ups each add a new angle (not "bumping this")
- ☐ Sequence ends with a graceful break-up email
- ☐ Sequences stop automatically on any reply

CADENCE

- ☐ Email + LinkedIn cadence mapped out (day by day)
- ☐ LinkedIn activity at human-like limits
- ☐ Every touch knows about every other touch
- ☐ Reply destination (landing page) converts the click

WEEKLY MONITORING

- ☐ Inbox placement tested across all active domains (95%+ target)
- ☐ Blacklists checked for all sending IPs and domains
- ☐ Bounce rate reviewed and hard bounces pruned

LIST & DATA

- Addresses verified: syntax → SMTP → catch-all risk scored
- Role accounts removed (info@, office@, sales@, admin@)
- Catch-all addresses sorted by decision tree (send/skip/verify)
- Suppression list built (existing customers, past prospects)
- Bounce target confirmed: under 1%
- Google / Yahoo compliance: unsubscribe header in place

- Positive reply rate vs. total reply rate tracked separately
- Domains below 90% placement flagged for review or rest
- Suppression list updated after every campaign
- New domain warmup on schedule for any volume expansion

TARGET METRICS

METRIC	TARGET	MOONGIE LIVE
Inbox placement	95%+	98.7%
Reply rate	3-5%	~4.5%
Bounce rate	<1%	~0.8%
Per-mailbox cap	25/day	25 (hard)
Warmup period	3-4 weeks	Never rushed

WANT THIS HANDLED FOR YOU?

Cold email that lands, managed end to end.

Moongie runs managed cold email infrastructure - domains, warmup, verified lists, copy tuning and daily deliverability monitoring - plus mixed email + LinkedIn outreach and the landing pages that convert the clicks.

You tell us what, why and to whom. We do the rest.

COLD EMAIL INFRASTRUCTURE

Dedicated or shared infrastructure, operated by us. Domains, warmup, authentication, daily monitoring. Never a self-managed handover.

MIXED OUTREACH

Email + LinkedIn running as one coordinated motion. Familiarity multiplies reply rates - we run the cadence across both channels.

ICP RESEARCH & LISTS

Verified, bounce-tested lists built to your ICP. Catch-all addresses handled deliberately. Data quality is a deliverability decision.

WEBSITES & LANDING PAGES

High-converting pages that catch the interest your inbox-placed emails earn. Live in 7 days. Outbound and conversion, treated as one system.

Book a free 30-minute strategy call or write to us directly:

moongie.com/contact

io@moongie.com · moongie.com