SELLERS DIRECTORY

A FREE GUIDE

The Cold Email Infrastructure Playbook

How to email 500 Amazon sellers a week without your domain getting nuked, your account getting suspended, or a German regulator sending you a love letter.

Updated April 2026

sellers.directory

FREE WITH EVERY ORDER

> So you've got a list. Maybe you pulled 500 German Amazon sellers from sellers.directory last week, maybe you have 2,000 contacts sitting in a CSV from somewhere else. Either way, you're staring at the file thinking *"now what?"*

This guide is for the person who has the leads and zero infrastructure. By the end of it you'll know exactly how to send cold email at scale without burning your main domain, getting your Google account suspended, ending up on a blocklist, or worst case landing in front of an EU data protection regulator.

Heads up before you start. This is a 3-week project. Not a weekend. Not an afternoon. Real cold email infrastructure takes about 21 days from "I bought a domain" to "the first email actually goes out", and roughly 25 to 35 hours of focused work spread across that window.

If you're up for that, keep reading. Everything is here. If you're not, skip to the end. There's another option.

WHAT'S INSIDE

Part 1. The legal layer

(Do this first or you'll regret it.)

I'm putting this section first because everyone wants to skip it, and the people who skip it are the ones who get a cease and desist six weeks in. Cold email is legal. Lazy cold email is not. The difference is twenty minutes of reading.

The four laws that apply to you

There are four pieces of legislation you need to know the names of. You don't need to read the full text. You just need to know what they require.

CAN-SPAM (United States). Sets the baseline for any email going to a US recipient. You need an accurate "from" name, a non-deceptive subject line, your physical mailing address inside the email body, and a working opt-out that's honoured within 10 business days. CAN-SPAM allows unsolicited B2B email. You don't need consent. You just need to play by the rules.

GDPR (European Union). This is the one that matters most for sellers.directory users, because the whole list is EU sellers. GDPR is stricter than CAN-SPAM but B2B cold email is *not banned* under GDPR. It's allowed under "legitimate interest". Meaning: if you can show that the recipient has a clear professional reason to want to hear from you, and you're emailing their business address (not personal), and you give them an easy way to opt out, you're inside the rules. A purchasing manager at an Amazon seller account being emailed by a B2B supplier is a textbook legitimate interest case.

PECR (United Kingdom). Sits on top of UK GDPR. Same B2B legitimate interest carve-out. The key difference: PECR is stricter about emailing sole traders and partnerships, treating them more like consumers. If your list includes UK one-person operations, treat those entries like you would a B2C contact and only email if they've opted in somewhere.

CASL (Canada). Strictest of the four. Canada actually does require some form of express or implied consent for commercial email, even B2B. If your list has Canadian recipients, segment them out and either skip them or use a different channel (LinkedIn, phone) to make first contact.

The non-negotiables

Regardless of which law applies to which contact, every cold email you send needs all of the following, every single time:

1. **A real, identifiable sender name.** "Sales Team" is not a name. "Sarah from sellers.directory" is.
2. **A non-deceptive subject line.** It can be casual, it can use spintax, it cannot lie about what's in the email.
3. **Your physical mailing address inside the email.** Yes, in every email. A registered business address works. A virtual office address works. A home address works (if you're brave). What doesn't work is no address.
4. **A working unsubscribe.** This can be a "reply with NO and I'll stop" line, which counts as a functional opt-out under CAN-SPAM and GDPR, or it can be a one-click link. Either way, when someone uses it, they come off the list within 24 hours. Not next week. Not when you remember.
5. **No misleading headers.** Your "from" address has to actually be from the domain you're claiming to send from. No spoofing.

The list-source rule

There's a difference between "data you scraped" and "data that was published for the purpose of being contacted in a business context". Public business contact information is the kind you find in a directory, on a company website's contact page, or in a B2B platform like sellers.directory where the contact is explicitly listed as the seller's business email. That falls into the second category. You can defend its use under legitimate interest.

A LinkedIn scrape doesn't fall into that category. Neither does a list of personal Gmail addresses bought from a sketchy reseller. If a regulator ever asks "where did you get this?", "I scraped LinkedIn" is not a defence. "I purchased it from a B2B marketplace that lists business contacts published by the businesses themselves" is.

This isn't a small distinction. It's the entire reason your sellers.directory list is safe to send to and a personal Gmail dump isn't. Don't mix them.

Part 2. Buying & setting up domains

Why you can't use your main domain

Picture this. You send 500 emails from `you@yourcompany.com`. Twenty bounce because the addresses were stale. Forty go to spam. Three people mark them as spam and click "report phishing". Your Google account flags `yourcompany.com` as a low-reputation sender. Suddenly your customer support inbox isn't reaching customers. Your invoices are landing in promotions tabs. Your team's calendar invites are getting filtered. One bad campaign permanently damages the domain you actually run your business on. There is no fix. There is no appeal. You just bought a new domain and started your business email life over.

This is why every cold email operator alive uses *separate* domains for cold outreach. Always. No exceptions.

How many domains you need

Quick math. Industry-safe limits are 100 emails per domain per day, 20 to 30 per individual mailbox per day. You want to send 500 emails a week, that's 100 a day across a five-day work week. So technically one domain could handle it. But you don't want one domain. You want three to five.

Why? Three reasons.

1. **Redundancy.** If one domain has a bad week and reputation drops, you rotate to the others while it cools off.
2. **Volume headroom.** When you scale from 500 a week to 1,000 a week, you don't want to be redoing all this DNS work.

3. **A/B testing.** Different domains can run different sequences, and you can compare reply rates without polluting the data.

> **Recommendation.** For a sellers.directory user starting from zero: **buy three domains.** Five if you're planning to scale fast.

What to buy

Don't buy your main domain plus a typo. `yourbiz.com` and `yuorbiz.com` look bad. They look like phishing, because that's how phishing operators do it. Buy *close lookalikes* that any reasonable person would understand are related variants:

- `.co` instead of `.com` (e.g. `yourbiz.co`)
- `.io` for tech-feeling brands
- A "get" or "try" prefix (`getyourbiz.com`, `tryyourbiz.com`)
- An "HQ" or "co" suffix (`yourbizhq.com`, `yourbizco.com`)
- The product name as the domain (`sellersdirectory.com` if your main is something else)

Buy them on **GoDaddy**, **Namecheap**, or **Porkbun**. Porkbun is the cheapest and has the cleanest interface. Namecheap is fine. GoDaddy works but they will spam-call you. All of them charge $10 to $15 per .com per year. Budget $50 for three domains, $75 for five.

Forwarding the root domain

Every alt domain you buy needs to redirect to your main website. Why? Because when a curious prospect copies the domain out of your email and pastes it into their browser, they need to land somewhere that looks like a real business. If they hit a "this site can't be reached" page, you look like a scammer. Set up a 301 redirect from each alt domain to your main site. Every domain registrar offers this in their dashboard for free. Takes about 30 seconds per domain.

Part 3. DNS records

(The part everyone screws up.)

This is the boring part. It's also where 80% of cold email sends die before they leave the building. There are four DNS records you need on every single domain you bought, and they all need to be perfect, and you need to wait 24 hours for them to propagate, and then you need to verify them before you trust them.

MX records

MX records tell the world which mail server handles email for your domain. You're using Google Workspace (we'll get to why in Part 4), so you need to point each new domain at Google's mail servers. Inside your domain registrar's DNS panel, add the following MX records:

```
Priority 1   ASPMX.L.GOOGLE.COM
Priority 5   ALT1.ASPMX.L.GOOGLE.COM
Priority 5   ALT2.ASPMX.L.GOOGLE.COM
Priority 10  ALT3.ASPMX.L.GOOGLE.COM
Priority 10  ALT4.ASPMX.L.GOOGLE.COM
```

Delete any default MX records the registrar pre-populated. Do this on every domain.

SPF: proving you're allowed to send

SPF (Sender Policy Framework) is a TXT record that lists which mail servers are authorised to send email "from" your domain. Without SPF, every email you send is going to land in spam, because the receiving server has no way to verify that the sender is legit.

Add this TXT record on the root of each domain:

```
Type:  TXT
Host:  @
Value: v=spf1 include:_spf.google.com ~all
```

The `include:_spf.google.com` part says "Google is allowed to send for me". The `~all` at the end means "anything not on this list, treat as suspicious but don't outright reject". Use `~all`, not `-all`, until you're confident everything is dialled in.

DKIM: signing your emails so they aren't tampered with

DKIM (DomainKeys Identified Mail) puts a cryptographic signature on every email you send so receiving servers can verify it actually came from you. To set this up:

1. Inside Google Admin (admin.google.com), go to **Apps → Google Workspace → Gmail → Authenticate email**.
2. Pick the domain you're setting up.
3. Click **Generate new record**. Choose 2048-bit. Click generate.
4. Google gives you a CNAME record. It looks like `google._domainkey` pointing at a long string starting with `v=DKIM1; k=rsa; p=...`.
5. Copy that into the DNS panel of your registrar as a TXT record.
6. Wait an hour. Come back to Google Admin and click **Start authentication**.

Verify it actually propagated by running `dig txt google._domainkey.yourdomain.com` from a terminal, or pasting the domain into mxtoolbox.com. If you don't see your record, you copied it wrong. (You probably copied it wrong. Everyone copies it wrong the first time.)

DMARC: telling receivers what to do with failed messages

DMARC sits on top of SPF and DKIM and tells the receiving server what to do if either of them fails. Start with a permissive policy and tighten it later.

```
Type:  TXT
Host:  _dmarc
Value: v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com
```

The `p=none` part means "don't reject anything yet, just monitor". After two weeks of clean sending, change it to `p=quarantine`. After another month, `p=reject` if you're feeling brave.

The 24-hour propagation wait

DNS changes don't apply instantly. They propagate across the internet over the course of anywhere from 15 minutes to 48 hours. Don't trust your records until you've verified them in mxtoolbox or with a `dig` command, and don't start sending until you've waited a full 24 hours after the last change.

Part 4. Buying mailboxes

Google Workspace, not regular Gmail

Consumer Gmail accounts (the free `@gmail.com` ones) are not allowed to be used for cold outreach. Google's anti-abuse systems will flag and suspend any consumer Gmail account that starts sending bulk cold mail. Even if you connect it to a sequencer, the suspension can happen in days. You will lose the account, the warmup time, and the reputation you built.

The only safe way to send cold email from a Google address is **Google Workspace**. The paid version, where Google has actually licensed your business to use your custom domain through their mail infrastructure. It's the same Gmail interface, but the rules are different and the rate limits are higher.

What it costs

Workspace seats run $6 per mailbox per month on the Business Starter plan. You want **two mailboxes per domain** (more on why in a moment). With three domains, that's six seats. With five domains, ten seats. Six seats × $6 = $36/month. Ten seats × $6 = $60/month. Just for the inboxes, before you've sent a single email.

Provisioning each seat individually

Inside Google Workspace admin, create each mailbox by hand. For each one, fill in:

- **A real first and last name.** Different for every mailbox. Use a name generator if you have to. Don't use "Sales Team" or "Outreach 1".
- **A handle.** `firstname@yourdomain.com` or `firstname.lastname@yourdomain.com`. Avoid `info@` or `hello@`, those look automated.
- **A profile photo.** A real, generated headshot (thispersondoesnotexist.com works) or a stock photo. Each mailbox needs to look like a real human if anyone clicks the avatar.
- **A recovery phone and recovery email.** You will need these if Google ever throws a security challenge.
- **A time zone matching the persona.** A "Hannah Schmidt" mailbox should be set to Berlin time, not Los Angeles.
- **A signature.** Plain text only. Name, role, company, mailing address (the legal one).

Why two mailboxes per domain? Because if one mailbox gets flagged, you have a backup. And because rotating across multiple mailboxes per domain spreads the load and makes the sending pattern look more organic.

The 72-hour cooldown

Brand new Google Workspace accounts can't go straight into a sequencer. Google needs to see the account behave like a normal mailbox for at least 72 hours before you start automated sending. During this window: log in from a normal browser, send a real email to a real friend, reply to something, file a message into a folder. Make it look used. Then leave it alone for three days. *Then* connect it to your warmup tool.

Part 5. Warmup (the 2-3 week wall)

What warmup actually is

Warmup is the process of building a sender reputation with Google's spam filter before you ever send a real cold email. It works by using an automated tool that has your fresh mailbox send small amounts of fake "conversational" email back and forth with other mailboxes in the warmup network. The recipient mailboxes auto-reply, mark messages as important, move them out of spam, and generally simulate the behaviour of a real human inbox. Over 2 to 3 weeks, this teaches Google that your mailbox is being used by a real person who sends and receives real conversations. Without it, your first cold email lands in spam and your domain reputation tanks instantly.

14 days minimum. 21 days preferred. No exceptions. I've seen people try to skip this. I've seen what happens. They send their first 50 cold emails on day 5 of warmup, get a 7% spam rate, and burn the domain in a week. The shortcut takes longer than the right path.

Tools that do this

- **Standalone warmup services** like Mailwarm and Warmup Inbox. Around $30 to $60 a month per mailbox.
- **Built-in warmup inside your sequencer.** Smartlead, Reachinbox, and Instantly all have warmup built into their main product. This is what most people use.
- **Lemwarm**, the original. Works fine, slightly more expensive.

The warmup ramp curve

Warmup tools let you set a daily volume. Don't set it to "max" on day one. Use this curve:

- Days 1 to 3: 5 warmup emails per day
- Days 4 to 7: 10 per day
- Days 8 to 14: 20 per day
- Days 15 to 21: 30 to 40 per day

By day 21, your mailbox has built up enough sender history that Google trusts it.

Inbox placement testing

Halfway through warmup (around day 10), and again at the end (day 21), run an inbox placement test using **GlockApps**. About $59 a month for the smallest plan, and worth every dollar. If you're sitting at 90% or higher primary placement, you're ready. If you're below 70%, do not start sending. Extend warmup another week and test again.

Part 6. List hygiene

(Or, how to not bounce yourself into oblivion.)

The 2% bounce rule

Google starts throttling your sender reputation when bounces exceed 2% of sends. At 5%, they stop delivering you to inboxes at all. Your bounce rate has to stay under 2% on every campaign. There is no margin for sloppiness.

Validating before you send

Before any list goes into a sequencer, run it through an email verifier. The two everyone uses are **NeverBounce** and **MillionVerifier**. Both charge around $0.005 per email, so a 1,000-contact list costs you $5 to validate. Cheap insurance.

Both tools return four categories:

- **Valid.** Keep them. These will deliver.
- **Invalid.** Delete them. These will bounce and hurt you.
- **Risky.** Skip them. The volume isn't worth the deliverability risk.
- **Unknown.** Skip these too.

After verification you typically lose 5% to 15% of a list. That's normal.

Suppression lists

Build a master suppression file from day one. Any time someone replies "no", any time someone bounces, any time someone unsubscribes, they go on the master suppression list. Before you upload any new campaign, run it against the suppression list and remove matches.

Part 7. Sending platform (pick one)

You need a sequencer. This is the tool that actually sends your emails on a schedule, manages replies, handles unsubs, rotates mailboxes, and tracks performance. Three real options.

Smartlead. $39 a month entry tier. Unlimited mailboxes on higher plans. Built-in warmup. Clean UI. Strong with high-volume operators. Probably the best value if you're scaling.

Reachinbox. Newer, similar feature set, slightly more polished interface. Good built-in warmup, integrated unified inbox, decent reporting.

Instantly. The most popular among agencies. Unlimited inbox plans, very strong warmup pool because so many users feed into it, simple UI. Slightly more expensive than the other two.

There is no "right" answer. Pick one based on price and which UI you like in a 10-minute demo. You can always switch later. Budget $100 to $150 a month for the sequencer subscription on top of your other infra costs.

Connecting your mailboxes

Inside your chosen sequencer, you connect each Google Workspace mailbox via IMAP and SMTP. This means:

1. Enable 2-factor authentication on the Google account. Mandatory.

2. Generate an **app password** in Google Account → Security → 2-Step Verification → App Passwords.
3. Paste the app password into the sequencer's connection screen, along with the username (the full email address) and the IMAP/SMTP server addresses (`imap.gmail.com` and `smtp.gmail.com`).
4. The sequencer will run a connection test. If it works, the mailbox shows up as "connected". If not, you used the wrong app password.

Part 8. Sending rules & limits

These limits aren't suggestions. They're the line between a campaign that lands and a campaign that gets you blocklisted.

20 to 30 emails per mailbox per day. Maximum. Going higher doesn't get you more replies, it gets you marked as a spammer faster.

100 emails per domain per day. Maximum. This applies even if you have five mailboxes on a single domain. Google evaluates reputation at the domain level.

Mailbox rotation. Inside your sequencer, attach all mailboxes from all domains to every campaign. The sequencer will distribute the day's sends evenly across them. 10 mailboxes × 25 emails a day = 250 emails a day across infrastructure.

Send windows. Tuesday, Wednesday, Thursday. 8am to 11am in the recipient's local time zone. Mondays and Fridays underperform. If your list spans multiple time zones, segment it and use different campaigns per region.

3 to 5 second delay between sends. Inside a single mailbox, don't fire emails back-to-back. Use a "human delay" setting of 3 to 5 seconds.

Part 9. Writing emails that don't trip filters

Spintax 101

Spintax is one of the most useful deliverability techniques nobody tells beginners about. The idea: instead of sending the exact same email to 500 people, you write the email with multiple alternative phrasings inside `{a|b|c}` markers. The sequencer randomly picks one variation per send. Every recipient gets a slightly different email, no two messages are byte-identical.

Subject line spintax:

```
{quick question|quick one|question for you|one for you}
```

Opener spintax:

```
hey {{first_name}}, does {{company}} {sell to|supply|work with} any
Amazon sellers in europe at the moment?
```

CTA spintax:

```
{worth a peek?|figured i'd flag it|could be worth a 60-sec look}
→ https://yourdomain.com
```

Aim for 2 or 3 spintax options on every sentence in the email. Twenty spintax slots in a 200-word email give you trillions of unique combinations.

The link problem

One link maximum per email. Two or more links is a known spam pattern. **No URL shorteners.** Bit.ly, t.co, tinyurl. Instant spam flag. **No tracking parameters.** No `?utm_source=cold&utm_campaign=outreach`. UTM tags trigger filters. Strip them.

No images, no HTML signatures, no attachments

Cold sequence emails are plain text. Period.

- **No images.** Image-heavy emails are flagged as marketing.
- **No HTML signatures.** Use a four-line plain text signature: name, role, company, address.
- **No attachments.** Anything attached to a cold email is suspicious. If you need to share a PDF, link to it on a real domain.

Personalisation tokens

Every sequencer supports merge tags: `{{first_name}}`, `{{company}}`, custom variables. Use them, but **always set fallbacks**. If your list has a row missing the first name field, the sequencer will literally send "hi ," and you'll feel it in the reply rate.

Open and click tracking off

In 2026, this is non-negotiable. Tracking pixels and click-tracked links are flagged by Apple Mail Privacy Protection, by Gmail's enhanced spam detection, and by basically every modern mail client. Turn off open tracking and click tracking on every cold campaign. You lose some metrics. You gain a 10% to 20% deliverability lift.

Part 10. Reply handling

Half the operators I've seen burn out do it because they didn't think through what happens when people actually reply.

Reply within 4 hours during business hours. Cold email is a momentum game. A positive reply that sits overnight cools by 60% by morning. Build a habit: open the unified inbox in your sequencer at 9am, 1pm, and 5pm. Reply to everything in there before closing the tab.

The "no" handling rule. When someone replies "no", "not interested", "remove", "stop", "wrong person", or any variation: instant suppression. Polite acknowledgement ("understood, taking you off the list, sorry for the noise"). Never argue.

Out-of-office detection. Most modern sequencers automatically detect OOO replies and pause the sequence for that contact. Make sure it's enabled.

The unsubscribe loop. Honour every opt-out within 24 hours, full stop. Run a manual review of your unified inbox once a week to catch anyone whose intent was clear but didn't use exact unsub language.

Part 11. Monitoring & ramping

Weekly deliverability check

Every Monday morning for the first six weeks: run a GlockApps inbox placement test. Three minutes of work. If primary inbox placement drops below 80%, pause sending and investigate.

Bounce, reply, unsub dashboard

The numbers you want to see, weekly:

- **Reply rate.** Above 2% positive, above 5% total.
- **Bounce rate.** Below 2%. Below 1% is great.
- **Unsubscribe rate.** Below 0.5%. Above 1% means your subject lines or opening sentence are misaligned with the list.

If any of these go sideways, stop sending and fix the cause before you send another batch.

The 90-day ramp plan

- **Month 1.** 100 emails a day total across all infrastructure. Build reputation. Watch numbers.
- **Month 2.** 200 emails a day. Add a domain or two more mailboxes if you need the headroom.
- **Month 3.** 300 emails a day. Now you're at "real volume", about 1,500 a week, around 6,000 a month.

Patience or pain. Pick one.

Part 12. The cost & time reality

So you've read all of that. Here's what it actually costs and how long it actually takes:

Item	Cost
3 to 5 domains (one-time)	$50 – $75
Google Workspace seats (6 to 10 mailboxes)	$36 – $60 / mo
Sequencer (Smartlead / Reachinbox / Instantly)	$100 – $150 / mo
Warmup (often bundled with sequencer)	$0 – $60 / mo
List validation (NeverBounce / MillionVerifier)	$25 – $50 / mo
Inbox placement testing (GlockApps)	$59 / mo
Recurring monthly total	**$220 – $380 / mo**

And the time:

- **Time to first email going out:** about 21 days from buying domains
- **Setup hours, focused work:** 25 to 35 hours
- **Ongoing maintenance:** about 5 hours a week

This is what real cold email infrastructure looks like in 2026. There is no shortcut that doesn't cost you a domain, a Google account, or a regulator complaint.

Part 13. The shortcut

Or, you could just hand it to us.

This is what most sellers.directory customers end up doing. You book a call with someone on our team and we set the whole thing up for you in about a week.

We buy the domains, configure the DNS records, provision the Google Workspace mailboxes, run the full warmup cycle, connect everything to a sequencer, and hand you back a working sending stack with your first campaign drafted in your voice.

You give us your sellers.directory list and a few sample emails in your tone. We give you back the keys.

Either path is fine. This guide works whether you do it yourself or hire it out. But if you'd rather skip the 25 to 35 hours of DNS records and Google Admin tabs, drop us a line: hello@sellers.directory.

— the sellers.directory team

This guide is updated quarterly as platform rules and best practices change. Last updated: April 2026.