

# The Notice-Channel Checklist

**The premise, in one line:** FMCSA contacts whatever is on file. If what's on file is wrong, you fail by silence, and failure to respond is treated as failure, full stop.

## The nine lines: DO-CONFIRM

**DO-CONFIRM.** Every line below is something you already believe is true, and that is exactly the problem: every documented version of this catastrophe turned on a contact field somebody would have sworn was current. So work from memory if you like; then stop and read the record itself. About 30 minutes on the record and 15 on the channel the first time through. After that it's a read, not a project.

**PAUSE POINT:** the day you file your biennial MCS-150 update, with the record open in front of you. That's the one date on this list that comes around on its own, which is what makes it the right hook to hang the rest on. If you've never run these nine lines, the pause point is today, and the update date takes over afterward.

- ☐ **1. Your MCS-150 as filed is open, and all four contact fields have been read one at a time:** mailing address, physical address, email, phone. Not "probably right." Read each one against reality.
- ☐ **2. The email on file is an inbox a current owner or manager actually opens,** not a former employee, not an old address nobody checks, not your authority filing service.
- ☐ **3. The phone on file is a real number somebody answers. Never a throwaway number entered to dodge vendor spam.** That's the number FMCSA, or the state trooper assigned your audit, will call.
- ☐ **4. The biennial MCS-150 update date is on the calendar.** You must file it at least every two years, whether or not anything changed. Put a reminder beside it to re-read these fields any time you move, change email systems, or change who runs the office.
- ☐ **5. .gov senders are whitelisted, and so is your state enforcement agency's domain.** Many audits are run by state partners whose addresses are **not** .gov, so the specific state DOT/DPS domain has to be on the list by name.
- ☐ **6. A monthly five-minute check of the FMCSA portal's Correspondence section is on the calendar.** Official notices land there regardless of what the mail carrier or the spam filter did.
- ☐ **7. Whoever opens the mail has been told, out loud:** government-looking letters about audits or compliance go to [name] the same day. Unopened junk-sort is how real notices die. When in doubt, hand it over.
- ☐ **8. You know what a real notice looks like when it lands.** Safety-audit contact comes from an FMCSA dedicated mailbox or the assigned state agency. So "not a .gov address" does **not** mean fake, and "looks official" does **not** mean real.
- ☐ **9. You never verify a letter or email using a link or a phone number printed in it.** You log in to the FMCSA portal directly, or you call FMCSA on the number published on [fmcsa.dot.gov](https://fmcsa.dot.gov).

**The scam line 9 defeats.** FMCSA's fraud alerts document a "fake safety audit" email that routes you to a look-alike portal harvesting your PIN, EIN, and Social Security number. FMCSA never charges for forms and never cold-calls through telemarketers. The defense isn't spotting a good forgery. It's that you only ever

verify through a channel the sender didn't hand you. Chapter 1's "Is the letter even real?" section carries the longer version, including why both mistakes cost money.

Nine boxes, and not one of them costs anything or needs software. They prevent the most expensive documented failure in this book, the one where nothing was wrong except that nobody could reach you.

**What done looks like:** every MCS-150 contact field verified this quarter · portal Correspondence check on the calendar · the mail-opener briefed · you can say out loud which address, inbox, and phone number the government believes is yours.