Supply Chain Solutions

Freight Fraud Identification Checklist

Use before releasing any load. Complete all applicable steps.

Strategic fraud (double brokering, identity theft, fictitious pickups) now accounts for roughly one-third of all cargo theft incidents. This checklist covers the **10 verification steps** that separate high-risk releases from protected ones.

SECTION 1: CARRIER & AUTHORITY VERIFICATION

Confirm you are working with a legitimate, active carrier before the load is tendered.

- ☐ **Verify carrier authority.** Confirm active MC/DOT number via FMCSA's SAFER database. Authority should be active — not pending or revoked.
- ☐ **Check operating history.** New authorities (under 6 months) and recently reactivated ones are high-risk. Cross-reference carrier age with load size and value.
- ☐ **Validate insurance.** Confirm active cargo and liability insurance with certificates that match carrier name exactly. Call the insurer directly if the load is high-value.
- ☐ **Verify safety rating.** Carriers rated 'Unsatisfactory' or with excessive out-of-service violations are red flags. Use FMCSA's SMS portal.
- ☐ **Flag suspicious bidding patterns.** A carrier bidding on loads far outside their normal geography, or claiming more trucks than FMCSA records reflect, warrants extra scrutiny.

SECTION 2: DRIVER & DISPATCHER IDENTITY

Impersonation is one of the fastest-growing theft vectors. Verify every person in the chain.

- ☐ **Verify driver identity.** Request a government-issued photo ID. Compare name against dispatch documentation. Do not release to anyone who cannot produce ID.
- ☐ **Confirm dispatcher information.** Call the carrier's verified phone number (not one provided in a new email) to confirm dispatcher identity independently.
- ☐ **Check email domain authenticity.** Fraudsters use spoofed domains that are one character off (e.g., 'supp1ychains.com'). Verify sender domains before acting on any load instructions.
- ☐ **Validate callback numbers.** If a dispatcher calls from a number that doesn't match the carrier's FMCSA record, verify before proceeding. VoIP and international call spoofing are common.

SECTION 3: PICKUP DETAILS & LOAD RELEASE

The dock is the last line of defense. These steps prevent freight from leaving with the wrong driver.

- ☐ **Verify pickup appointment.** Confirm the driver's name, truck number, and arrival window match what was scheduled. Early arrivals with no advance notice are a common red flag.
- ☐ **Cross-check BOL details.** Confirm shipper name, consignee, commodity, piece count, and seal number match the original bill of lading before loading begins.
- ☐ **Confirm tracking is active.** Ensure the carrier's tracking or ELD system is live and accessible before releasing. A carrier who cannot provide tracking access warrants a hold.
- ☐ **Flag last-minute carrier changes.** A sudden carrier swap close to pickup is one of the most reliable signals of double-brokering fraud. Require re-verification from scratch on any change.
- ☐ **Follow theft-prevention protocols for the lane.** High-risk lanes (Southern California, Texas Triangle, Metro Atlanta, Chicago) warrant additional verification steps and documentation.

⚠ STOP AND ESCALATE: Common Red Flags

- Driver arrives early with no advance notice
- Carrier insists on using their own BOL
- Requests to skip verification 'due to urgency'
- New carrier authority (under 6 months) on a high-value load
- Phone number or email domain doesn't match FMCSA records
- Last-minute dispatcher or driver substitution
- Carrier cannot provide active tracking
- Pickup location differs from scheduled address