D74 TECHNOLOGIES

Operational Methodology for Carrier Fraud Prevention

A D74 Technologies Whitepaper

Yevgeniy Melnik
Founder, D74 Technologies

D74-WP-2026-05 · PUBLIC EDITION
MAY 2026

Table of Contents

Purpose & Whitepaper Overview

Executive Summary

Cargo fraud succeeds where vetting stops and conversation begins. This whitepaper documents the operational layer that sits between a broker's compliance checks and a load leaving the dock: three Standard Operating Procedures (incident response, social engineering defense, warehouse release) and two framework primers (real-time deception detection, sold-MC behavioral drift). Methods are scale-independent, ready to apply by working teams, and designed to extend — not replace — the TIA Framework to Combat Fraud.

Purpose

This whitepaper documents operational methodology for preventing freight fraud at the points where it most often succeeds: the carrier vetting conversation, the dock release decision, and the first hour after a suspected theft. It contains three Standard Operating Procedures and two framework primers, drawn from twelve years of operational experience in freight and refined through the Zero Trust Freight Security Framework developed by D74 Technologies.

The methods are designed to be applied directly by working brokers — not adapted, not interpreted, not consultancy-mediated. Print the checklists. Run the role-play exercises. Use the phrase tables during live calls. The material is operational, not aspirational.

Who This Is For

- **Carrier reps** — the people who pick up the phone first and decide what information to release
- **Risk and compliance managers** — the people accountable when fraud succeeds
- **Operations leads** — the people who run the first-48-hours response when a load goes missing
- **Brokerage and 3PL leadership** — the people deciding which procedures their teams operate to

The methods apply to brokerages of any size. The phrase tables, verification gates, and response phases are scale-independent.

What's Inside

#	Document	Operational use
1	**SOP 1 — First 48 Hours: Incident Response Playbook**	Six-phase response protocol covering containment, evidence preservation, law enforcement engagement, external notifications, active recovery, and post-incident review. Designed for the first call after a load is suspected missing or compromised.
2	**SOP 2 — Social Engineering Red Flags & Information Protection**	Seven categories of fraudster phrase patterns with safe-response scripts. Information classification: what never to share before verification, what shares after vetting, what is safe to share during inquiry.
3	**SOP 3 — Warehouse Release Protocol — Pre-Pickup Verification**	Three-phase pre-pickup verification protocol covering driver verification, loading monitoring, and seal verification. Includes the dual-door binding requirement, ISO 17712 strength rating standards, and the hand-the-phone verification technique for high-uncertainty calls.
4	**Primer A — AVP: Human-Layer Deception Detection**	Three-step conversation method (Ask → Validate → Probe) for surfacing deception in real time across dispatcher calls, driver verification, in-transit check-ins, and delivery confirmation.
5	**Primer B — Detecting Sold MCs Through Behavioral Drift**	Six behavioral signals that surface a sold or compromised MC (the same phenomenon — a legitimate MC whose operations have changed hands or been quietly subverted) before the first fraudulent load completes. Includes capacity ratio analysis (OTR versus local fleet baselines), cross-MC infrastructure overlap detection, and the trusted-carrier ninety-day re-verification standard.
6	**Related Industry Resources**	How this whitepaper sits alongside existing industry and government guidance — the TIA Framework to Combat Fraud, FBI IC3, FMCSA NCCDB and Motus, and industry data partners — and the operational layer it adds on top.

About D74 Technologies

D74 Technologies builds fraud-prevention intelligence for freight — carrier, facility, and broker OSINT that surfaces the gap between what a counterparty claims and what it actually is. The methodology in this whitepaper is drawn from the Zero Trust Freight Security Framework, D74's proprietary operational framework for freight security.

The author, Yevgeniy Melnik, spent twelve years in freight — driver, broker, operations manager, warehouse manager, security consultant — before founding D74. The methods described here were developed in that operational career and have been refined through red-team exercises against working broker teams. They are presented as ready-to-apply procedures, not theoretical recommendations.

Terms of Use

This whitepaper documents operational methodology developed by D74 Technologies. The Standard Operating Procedures are the work product of D74 Technologies. The framework primers (A and B) are excerpts from the Zero Trust Freight Security Framework, the proprietary intellectual property of D74 Technologies.

- **Permitted:** Internal use by the recipient organization for training, procedure development, and operational application.
- **Requires written permission from the author:** Incorporation as integrated content into other materials, derivative works, commercial training programs, third-party publications, or commercial products.
- **Attribution required:** "Yevgeniy Melnik / D74 Technologies" must be preserved in any subsequent use or republication.
- **Not permitted without permission:** Republication outside the recipient organization, removal of attribution, or commercial use by parties other than the recipient.

Contact for licensing or permission inquiries: yevgeniy@d74.io

All material in this whitepaper was developed by Yevgeniy Melnik / D74 Technologies. The framework primers are excerpts from the Zero Trust Freight Security Framework © D74 Technologies. The Standard Operating Procedures and primers were finalized for industry distribution in May 2026.

SECTION 1

SOP 1: First 48 Hours

Section 1 — SOP 1: First 48 Hours

Incident Response Playbook

D74 Technologies Whitepaper — Operational Methodology for Carrier Fraud Prevention
Prepared by Yevgeniy Melnik | May 2026

Purpose

Enable freight broker teams to respond rapidly, lawfully, and decisively to fraud, cargo theft, or high-risk red flags — with specific guidance on law enforcement engagement, evidence preservation, and the critical "first 48 hours" window where recovery is still possible.

Why "First 48" Matters

Law enforcement prioritizes cases with fresh evidence and active leads. After 48 hours:

- GPS/tracking data may be overwritten or unavailable
- Cargo is likely transferred, repackaged, or sold
- Witnesses forget details
- Jurisdiction becomes harder to establish
- Your case joins the queue of "85 cases ahead of yours"

The goal: Compress critical actions into the first 48 hours to maximize recovery chances and build a case that law enforcement will actually pursue.

Activation Triggers

Trigger this playbook immediately if ANY of the following occur:

Trigger	Examples
Load missing or stolen	No delivery, driver disappeared, trailer found empty
Seal broken, missing, or mismatched	Seal number doesn't match BOL, evidence of tampering
Driver identity in question	Different driver than dispatched, fake ID, phone number changed
POD manipulated or forged	Signatures don't match, timestamps altered, location spoofed
Tracking breaks unexpectedly	ELD goes dark, driver unreachable, last ping in unexpected location
Corridor deviation + abnormal behavior	Known lane broken, driver evasive about location
Double brokering discovered	Load re-brokered without authorization
Trusted carrier abuse suspected	Established carrier acting out of pattern
Impersonation confirmed	Someone posed as legitimate carrier/driver

Default rule: When in doubt, activate. Better to stand down than miss the window.

Response Team — Role Assignments

Role	Primary Responsibility	Backup
Carrier Rep	Detects red flags, initiates escalation, first documentation	After-hours on-call
Operations Lead	Coordinates operational response, communication hold	Branch Manager
Risk/Compliance Manager	Owns investigation, coordinates external notifications	Compliance Lead
Legal Contact	Reviews external communications, advises on liability	Internal counsel only
Executive Sponsor	Approves law enforcement escalation, client notification	Designated backup

Critical: Assign names and phone numbers to each role BEFORE an incident. During a crisis is not the time to figure out who owns what.

Phase 1: First 15 Minutes — Containment

Objective: Stop the bleeding. Preserve evidence. Don't tip off the suspect.

Immediate Actions

- [ ] **STOP all communication with the carrier/dispatcher** — Do not call, text, or email. Any contact may tip them off that you're aware.
- [ ] **Lock internal records** — Flag the load in TMS as "Under Investigation." Prevent edits or deletions.
- [ ] **Export current data immediately:**
- GPS/tracking screenshots (with timestamps)
- Last known location
- ELD data if available
- All communication logs (calls, texts, emails)
- [ ] **Log the detection:**
- Timestamp of when issue was discovered
- Who discovered it
- Initial summary of what's known
- Carrier rep name
- [ ] **Notify Operations Lead + Risk Manager** — Phone call, not email. Get confirmation they received it.

Do NOT:

- Call the driver or dispatcher to "check on the load"
- Post anything on Highway, DAT, or public systems yet
- Contact the shipper or client yet
- Discuss on Slack/Teams where others can see

Phase 2: First Hour — Evidence Preservation & Internal Review

Objective: Build the case file. Identify what you have and what's missing.

Evidence Collection Checklist

- [ ] **Pickup documentation:**
- Seal verification photos
- Trailer number photos
- Driver ID photo (if captured)
- BOL with signatures

- [ ] **Carrier file:**

- MC authority verification (screenshot from FMCSA)
- Insurance certificate
- W-9
- Carrier packet / onboarding documents
- Rate confirmation (signed)

- [ ] **Communication records:**

- All emails with carrier/dispatcher
- Phone call logs with timestamps
- Text messages
- Any voicemails (save audio files)

- [ ] **Tracking data:**

- Full GPS history export
- ELD records if available
- Macropoint / Project44 / FourKites data
- Screenshots of tracking at key points

- [ ] **Red flag history:**

- Previous issues with this carrier
- Any alerts from Highway / DAT
- Internal notes from vetting

Internal Analysis

- [ ] Check if dispatcher email/phone appears on multiple MC profiles
- [ ] Verify MC# matches the carrier who picked up
- [ ] Check for recently transferred MC (sold MC pattern)
- [ ] Review: Did we follow our own vetting SOP, or was it bypassed?

Phase 3: Law Enforcement Engagement

The jurisdiction problem: Freight crimes cross state lines. No single agency "owns" the case. This is why most cases get deprioritized.

Jurisdiction Decision Tree

Scenario	Primary Jurisdiction	Secondary
Theft at pickup location	Local PD where pickup occurred	State Highway Patrol
Theft during transit (location known)	PD/Sheriff where trailer last confirmed	FBI if interstate
Theft discovered at delivery (empty trailer)	Local PD at delivery	FBI if interstate
Location unknown	FBI (interstate theft)	State where carrier is domiciled
High-value cargo ($100K+)	FBI directly	State AG
Multiple thefts, same actor	FBI (pattern/RICO)	—

How to Get Law Enforcement to Act

The problem: Saying "I think my load was stolen" gets you a case number and nothing else.

The solution: Present a complete, organized case that requires minimal work from the officer.

What to prepare BEFORE calling:

1. **One-page incident summary:** - Load ID, pickup date/time, delivery date/time - Pickup address, delivery address - Last known location with timestamp - Cargo description and value - Carrier name, MC#, DOT# - Driver name (if known), truck/trailer numbers - Timeline of what happened
2. **Evidence packet (digital folder, ready to share):** - All photos - GPS/tracking export - Communication logs - Carrier documents - Rate confirmation and BOL
3. **Clear statement of crime:** - "Cargo valued at $X was stolen" — not "I think something happened" - Specific statute if known: **18 U.S.C. § 659** (Theft from Interstate Shipment) — the primary federal cargo theft statute, $1,000 sentencing-tier threshold. **18 U.S.C. § 2314** (Interstate Transportation of Stolen Property) may also apply if proceeds cross state lines, $5,000 threshold.

When you call:

> *"I'm reporting a cargo theft. The load was picked up at [address] on [date], bound for [destination]. The trailer was last tracked at [location] at [time]. The cargo is valued at approximately $[amount]. I have a complete evidence packet including GPS data, photos, and carrier documentation ready to provide. What's the best way to send this to you?"*

Key phrases that get attention:

- "I have GPS data showing the last location"
- "I have photos of the driver and truck"
- "The cargo value is over $100,000" (FBI typically prioritizes higher-value cases faster)
- "This carrier has multiple victims" (pattern = priority)
- "I can send you a complete case file right now"

CargoNet — A Force Multiplier

What: CargoNet operates a national database and information-sharing system for cargo theft incidents, connecting freight industry stakeholders with law enforcement agencies and crime analysts. Services are provided free of charge to law enforcement.

Why use them: They know which detective handles cargo theft in each jurisdiction. You don't.

How:

1. File a report with CargoNet immediately (even before local PD if load is still moving)
2. They will route to the correct agency
3. They track recovery and coordinate across jurisdictions
4. Their involvement signals to LE that this is real

Contact: 888-595-CNET (2638) · cargotheft@cargonet.com · cargonet.com

GenLogs — Roadside Sensor Network

What: A roadside sensor and camera network that has captured 3.4 billion images of commercial vehicles, with 15 million new images added daily. Observes 99% of active motor carriers regularly. Captures unique vehicle markings beyond what license-plate recognition alone provides — especially useful when chameleon carriers, mid-transit equipment swaps, or unmarked trucks are involved.

Why use them: GenLogs has provided more than 500 free investigations for the freight industry — and counting. For brokers and shippers, they provide real-time sighting data with photographic proof — timestamped imagery that can place a specific truck on a specific stretch of road at a specific time.

When to use them:

- Active recovery — a load is in motion and you need to locate it
- Post-theft recovery requiring evidence of when and where a vehicle was last seen
- Chameleon carrier investigation — when you suspect the same physical truck is operating under multiple MCs
- Confirming or refuting a driver's claimed location with photographic evidence

How:

1. Contact via email: contact@genlogs.io
2. Provide the trailer/truck identifiers, MC number, last known location, and theft window
3. They will pull sighting data from their roadside sensor network and return timestamped imagery where available

Pair with CargoNet: CargoNet handles law enforcement routing across jurisdictions. GenLogs handles asset locating through their physical sensor network. The two are complementary — use both for high-value or active-recovery scenarios.

FBI Cargo Theft Task Force

For interstate theft, high-value cargo, or repeat offenders:

- FBI generally prioritizes cases over $100,000
- File an IC3 complaint online: ic3.gov
- Primary reference: **18 U.S.C. § 659** (Theft from Interstate Shipment) — the cargo-specific federal statute. Secondary: **18 U.S.C. § 2314** (Interstate Transportation of Stolen Property) for proceeds crossing state lines.

Phase 4: External Notifications

Timing matters. Notify in this order:

1. CargoNet (Immediate — within first hour if load in motion)

- Provides law enforcement routing
- Broadcasts to recovery network
- Required by some insurance policies

2. Law Enforcement (Immediate — within first hour, in parallel with or via CargoNet)

- See **Phase 3: Law Enforcement Engagement** above for jurisdiction decision tree, what to prepare before calling, key phrases that get attention, and the engagement playbook
- CargoNet can route to the correct agency if you don't know which jurisdiction owns the case
- For interstate theft or high-value cargo, FBI / IC3 can be engaged directly
- Filing an LE report within the first hour establishes the case record and starts the recovery clock

3. Insurance Carrier (Within 2-4 hours)

- Check your policy for notification requirements
- Many policies require notification within 24-48 hours
- Provide incident summary and evidence packet
- Ask: "What documentation do you need from us?"

4. Client/Shipper (Within 4-8 hours, after you have facts)

- Use neutral, factual language
- Do NOT speculate or assign blame
- Provide: What happened, what you're doing, next update timeline

Template:

> *"We are investigating an incident involving load [ID] picked up on [date]. The shipment has not arrived as scheduled and we have engaged law enforcement and our recovery resources. We will provide an update by [time]. Please contact [name] at [phone] with any questions."*

5. Industry Databases (After internal validation — 24-48 hours)

Only flag publicly when you have confirmed:

- The carrier/driver committed fraud (not just a miscommunication)
- Your evidence is solid
- Legal has approved

Where to report:

- Highway — Flag carrier in system
- DAT — Report to compliance
- TIA Watchdog — Validated fraud reporting via TIA member portal
- CargoNet — If not already filed
- FMCSA NCCDB — Formal complaint channel for authority violations (nccdb.fmcsa.dot.gov · 1-888-368-7238)

Warning: Premature public flagging can expose you to defamation claims. Validate first.

Phase 5: If Load Is Still In Motion — Active Recovery

Note on Phase 1's no-contact rule: Phase 5 actions do not reverse Phase 1's directive to halt communication with the carrier/dispatcher. The goal here is different — to surface whether the driver answering a packet-verified number is the real driver. The carrier/dispatcher chain remains under no-contact until verification or law enforcement directs otherwise.

Time is critical. These actions happen in parallel with Phases 1-3.

Immediate Actions (within 15-45 minutes)

- [ ] **Engage GPS/tracking provider support** — Can they ping more frequently? Remote disable?
- [ ] **Attempt driver contact using VERIFIED number only:**
- Use the number from carrier packet, not what dispatcher gave for this load
- If different driver answers → red flag confirmed
- [ ] **File CargoNet report immediately** — They can broadcast to LE in the load's current area
- [ ] **Consider third-party recovery services:**
- Some insurers have recovery teams
- Private investigation (PI) firms specializing in cargo recovery
- Only with executive approval (cost)
- [ ] **Route diversion (if you have communication with real driver):**
- Divert to secure location
- Do NOT have driver confront anyone

If High-Value Cargo + Confirmed Theft

- [ ] Executive approval for law enforcement escalation
- [ ] Contact FBI directly (don't wait for local PD routing)
- [ ] Consider media blackout — don't tip off thieves that you're tracking

---

Phase 6: Post-Incident Review (Within 48-72 Hours)

Objective: Learn from the incident. Prevent recurrence. Feed the intelligence loop.

Incident Report (Required)

Field	Content
Incident ID	Unique identifier
Date/time discovered	When you first knew
Date/time reported to LE	When police were contacted
Carrier name / MC# / DOT#	Entity involved
Driver name (if known)	—
Cargo type / value	What was lost
Recovery status	Recovered / Partial / Total loss
Root cause	How did this happen?
Detection method	How did we discover it?
SOPs followed?	Which procedures were used or bypassed?
Lessons learned	What would we do differently?

Review Meeting Agenda

1. **Timeline reconstruction** — What happened, when?
2. **Red flags missed** — What should we have caught earlier?
3. **SOP gaps** — Where did our process fail?
4. **Carrier vetting review** — How did this carrier get approved?
5. **Action items** — What changes are we making?

Feed the Loop

- [ ] Update internal fraud database with carrier/driver info
- [ ] Share anonymized case summary for team training
- [ ] Update vetting criteria if a pattern emerged
- [ ] Report to TIA fraud reporting channels (Watchdog or equivalent), anonymized, for industry learning

---

Quick Reference — Contact Numbers

Resource	Contact	When to Use
CargoNet	888-595-CNET (2638)	Immediately for theft/recovery
GenLogs	contact@genlogs.io	Active truck/trailer locating, photographic sighting evidence, chameleon-carrier investigation
FBI IC3	ic3.gov	Interstate theft, high-value
FMCSA NCCDB	nccdb.fmcsa.dot.gov · 1-888-368-7238	Authority violations (NCCDB is the formal complaint channel)
TIA Watchdog	Via TIA member portal	Validated fraud reporting
Highway	Support via platform	Carrier flagging
DAT Compliance	Via platform	Carrier flagging

Appendix: Evidence Checklist (One-Page)

Print this. Keep it at every desk.

Immediately (First 15 min):

- [ ] Screenshot GPS/tracking with timestamp
- [ ] Export communication logs
- [ ] Lock TMS record
- [ ] Log who discovered, when, what

Within First Hour:

- [ ] Pickup photos (seal, trailer, driver)
- [ ] BOL with signatures
- [ ] Rate confirmation
- [ ] Carrier packet (MC, insurance, W-9)
- [ ] Full tracking history export
- [ ] Email/phone records

For Law Enforcement:

- [ ] One-page incident summary
- [ ] Evidence folder (organized, labeled)
- [ ] Cargo value documentation
- [ ] Timeline of events

Document Control

Version	Date	Author	Changes
1.0	May 2026	Y. Melnik	D74 Technologies whitepaper publication

This playbook is a response framework — not legal advice. All external actions should align with your company's legal policies and insurance requirements.

SECTION 2

SOP 2: Social Engineering Red Flags

Section 2 — SOP 2: Social Engineering Red Flags

Information Protection Guide

D74 Technologies Whitepaper — Operational Methodology for Carrier Fraud Prevention
Prepared by Yevgeniy Melnik | May 2026

Purpose

Arm broker teams with a recognition guide to spot and neutralize social engineering attempts before they succeed. This SOP covers:

1. **Red flag phrases** — What fraudsters say to extract information
2. **Information protection** — What should NEVER be shared before booking/vetting
3. **Safe responses** — How to deflect without losing legitimate business

---

Why This Matters

Fraudsters don't hack systems — they hack people. A single phone call can extract:

- Pickup number (PU#)
- Shipper address
- Consignee name
- Commodity type and value
- Dock contact names
- Load timing

With this information, they can:

- Impersonate a legitimate carrier at pickup
- Arrive early and steal the load
- Target high-value shipments specifically
- Build a profile for future attacks

The disclosure problem: In red-team exercises we've run against broker teams, a substantial majority disclosed sensitive information when asked the right way. The attack isn't sophisticated — it's social.

Information Classification

NEVER Share Before Verified Booking

Information	Why It's Dangerous
Pickup number (PU#)	Final key needed to pick up freight — often the only verification at the dock
Shipper facility address	Allows fraudster to show up and attempt pickup
Consignee name/ address	Used to reverse-engineer shipper identity or target specific receivers
Commodity type	Determines if load is worth stealing (electronics, pharma, alcohol = high value)
Exact weight/pallet count	Indicates value, ease of theft, consolidation potential
Dock contact names	Used to impersonate or social engineer facility staff
Rate confirmation	Contains PU#, addresses, commodity — everything they need

Share Only AFTER Vetting Complete

Information	When to Share
PU#	After carrier verified, rate con signed, tracking confirmed
Shipper address	After carrier verified, rate con signed
Commodity (general)	After carrier verified, if operationally necessary
Dock contact	After carrier verified, during active load

Safe to Share During Initial Inquiry

Information	Notes
General lane (city to city)	"Chicago to Dallas" — no specific addresses
Equipment type	"Dry van" / "Reefer" — not commodity details. **Hazmat exception:** must be disclosed (carrier needs HM endorsement), but treat as elevated risk — verify HM authorization before sharing further details
General rate range	If discussing terms

Note on dates: Pickup and delivery dates/times must be shared accurately during inquiry — real freight operations require precise scheduling. The protection isn't date-vagueness; it's that PU#, addresses, and rate confirmations are not released until carrier verification is complete.

Red Flag Phrases — Recognition Guide

Category 1: Urgency Pressure

Tactic: Create time pressure to bypass vetting steps.

Phrase	Why It's Dangerous	Safe Response
"I have a driver nearby, give us the info and we'll roll."	Pressures you to skip vetting because the "driver is ready"	"Great. Once we complete carrier verification, we'll send details."
"Just email us the rate con — our driver is on standby."	Attempts to get rate con (with PU# and addresses) before vetting	"We'll send the rate con after we verify your authority and insurance."
"I'm about to head home, send me the PU# so I can dispatch and be done for the day."	Uses personal urgency to rush you	"I understand. We'll have everything ready once verification is complete."
"We need to know NOW or we'll have to pass."	False scarcity to pressure quick decision	"No problem. Let me know if you'd like to proceed with verification."
"The shipper called us directly — we just need you to confirm the PU#."	Claims shipper relationship to bypass broker	"All pickups go through our dispatch. Let's complete verification first."

Pattern: Urgency + request for PU#, address, or rate con = red flag.

Category 2: False Familiarity

Tactic: Claim prior relationship to lower your guard.

Phrase	Why It's Dangerous	Safe Response
"We've worked with this shipper before, just send the PU#."	Implies relationship to skip verification	"Great — let me pull up your history. What's your MC number?"
"We've moved freight for you before — check your history."	Bluff relying on you not actually checking	"Let me verify that. MC number please?" (Then actually check)

Phrase	Why It's Dangerous	Safe Response
"We're calling on behalf of Carrier X — I'm the night dispatcher."	Claims association with known carrier	"I'll need to verify with the primary contact on file for that MC."
"Your colleague [name] usually sends us loads."	Uses a name to imply internal relationship	"Let me check with them. What's your MC number?"
"We're already in your system."	Assumes you'll take their word for it	"Perfect — let me pull up your profile. MC number?"

Pattern: Claimed familiarity + resistance to verification = red flag.

Rule: If they say "you know us," verify. If they're legitimate, they won't mind.

Category 3: Commodity Probing

Tactic: Extract commodity type to identify high-value targets.

Phrase	Why It's Dangerous	Safe Response
"What's the commodity? We need to know if it requires load bars."	Sounds operational, but probing for product type	"Standard dry freight. Your equipment handles it." *
"Is it electronics or food? Just so we can send the right trailer."	Directly asking for commodity category	"Dry van appropriate. Equipment requirements are on the rate con after booking."
"We just need to know the commodity to make sure it's covered under our policy."	Disguised as insurance compliance	"Your cargo policy covers general freight. We verify coverage during onboarding."
"Our insurance company is strict — we've been burned before. Can you share the commodity just to confirm?"	Sympathy play to extract information	"We verify insurance during carrier setup. What's your MC?"
"Do you know if it needs straps, bars, or blanket wrap?"	Probing for fragility/ value indicators	"Standard securement. Details on the rate con." *
"Can you confirm if it's hazmat or needs any endorsements?"	Backdoor to open commodity discussion	"No hazmat. Standard freight." *
"Just between us — what is it really? We've seen these loads go out under 'general freight' before."	Building false rapport to extract info	"It's general freight. Let's proceed with verification." *

*** Important — when the freight is NOT standard:** These responses assume the load is genuinely standard dry/general freight. Two exceptions:

- **Hazmat:** Must be disclosed — carrier needs the HM endorsement to even be eligible. But verify the carrier's HM authorization (and any required endorsements for the specific hazard class) before sharing any further details. Treat the entire interaction as elevated risk.
- **Specialized securement (load bars, straps, blanket wrap, climate control, oversize/overweight):** Equipment requirements can be discussed at a general level after carrier verification — the carrier needs enough information to confirm they can handle the load. Commodity-level detail (what's actually in the trailer) is not operationally necessary at the inquiry stage for standard dry freight and can wait until booking. Once the load is booked, full commodity disclosure happens normally through the rate confirmation and BOL.

Pattern: Multiple commodity questions + legitimate-sounding reasons = red flag.

Category 4: Consignee Extraction

Tactic: Get delivery location to reverse-engineer shipper or target specific facilities.

Phrase	Why It's Dangerous	Safe Response
"We can't book without knowing the consignee — if it's Walmart, we won't wait all day."	Uses operational concern to extract receiver identity	"Delivery is in [city]. Appointment details come with rate con."
"We're double booked — we need to confirm the consignee so we know which driver to send."	Misdirection to extract consignee	"I'll confirm driver assignment after we verify your carrier profile."
"Is it direct to DC or going to a 3PL?"	Probing for consignee type	"Delivery details on the rate con after booking."
"What's the delivery window? We need to know if it's a retailer with strict appointments."	Fishing for consignee indicators	"Delivery is flexible / appointment required. Details after booking."

Pattern: Consignee questions before commitment to the load = red flag.

Category 5: Contact/Name Fishing

Tactic: Get names to impersonate during pickup or delivery.

Phrase	Why It's Dangerous	Safe Response
"We're with dispatch — can you confirm who to talk to on the dock?"	Fishing for names to impersonate	"Dock contact is on the BOL. You'll receive that at pickup."
"Who should our driver ask for when he arrives?"	Same — fishing for names	"Check in with shipping/receiving. They'll have the paperwork."
"Can I get your direct number in case the driver has questions?"	Building contact profile	"Driver can call our dispatch line. That number is on the rate con."
"Who's the shipper contact? Just in case of delays."	Fishing for shipper-side names	"We handle shipper communication. Call us with any issues."

Pattern: Name requests before load is booked = red flag.

Category 6: Weight/Size Probing

Tactic: Determine if load is easy to steal, consolidate, or hold hostage.

Context — FTL vs LTL: These questions are red flags for **FTL (Full Truckload)** shipments — when the truck is dedicated to one shipment, weight and pallet count have no operational basis for the carrier, so the questions themselves are suspicious. For **LTL (Less Than Truckload)**, weight and pallet count are legitimate pricing and space-allocation data that must be shared during quoting; adjust responses accordingly while still withholding PU#, addresses, and commodity specifics until carrier verification is complete.

The responses below assume FTL context.

Phrase	Why It's Dangerous	Safe Response
"Can you confirm the weight? We're planning consolidation and need exact numbers."	May indicate illegal consolidation intent	"Weight is on the rate con. Approximately [X] lbs."
"We need the weight and pallet count to check if our team drivers can haul it under HOS."	Manipulates HOS logic to extract details	"Full truckload, within legal weight. Details on rate con."
"How many pallets? We want to make sure we have room."	Probing for size/value	"Standard load. Rate con has specifics."
"Is it light or heavy? Just making sure on equipment."	Probing for consolidation potential	"Standard weight for the equipment type."

Category 7: Channel Switching

Tactic: Move to less monitored communication to bypass security.

Phrase	Why It's Dangerous	Safe Response
"Can you text me the shipper address real quick?"	SMS is less monitored, easier to act on quickly	"All load details go through email or TMS. What's your email?"
"Just WhatsApp me the details."	Moving to unmonitored channel	"We communicate through official channels only."
"Send it to my personal email — our company server is down."	Attempting to bypass company records	"We only send to verified company email addresses."
"Call me back on this number, not the one on file."	Separating from verified contact	"I'll use the number we have on file for your MC."

Pattern: Request to switch channels + urgency = red flag.

Response Framework

The Verification Loop

When you hear a red flag phrase, use this response pattern:

1. **Acknowledge** — Don't be confrontational
2. **Redirect to verification** — "Let me pull up your profile"
3. **Request MC#** — Forces them to commit to an identity you can verify
4. **Verify before sharing** — Check FMCSA, your TMS, Highway/DAT

Example:

> ***Them:*** *"We've worked with you before, just send the PU#."*
>
> ***You:*** *"Great, let me pull up your history. What's your MC number?"*
>
> ***Them:*** *[Gives MC or gets evasive]*
>
> ***You:*** *[Verify MC in system before ANY information is shared]*

If They Push Back on Verification

Their Response	What It Means	Your Response
"We don't have time for this."	Red flag — legitimate carriers understand verification	"I understand. Once verified, we can move quickly."
"Your colleague doesn't make us do this."	Trying to create internal conflict	"This is our standard process for all loads."
"Forget it, we'll find another broker."	Testing if you'll cave	"No problem. Good luck." (Let them go)
"Fine, here's our MC."	Legitimate carrier	Proceed with verification

Rule: Legitimate carriers don't fight verification. Fraudsters do.

Escalation Triggers

Log the interaction and notify your supervisor if:

- Caller becomes aggressive when asked for MC#
- Multiple red flag phrases in one conversation
- Caller claims internal relationships that don't check out
- Caller requests channel switch after you decline to share info
- Something feels wrong — trust your instinct

Document:

- Time of call
- Phone number (check caller ID)
- MC# claimed (if any)
- What they asked for
- What was said

Training Exercise: Role Play Scenarios

Use these for team training:

Scenario 1: The Urgent Driver

> *"Hey, I've got a driver 20 minutes from your shipper in Memphis. He can grab that load right now if you send me the PU#. Otherwise we'll have to pass."*

Red flags: Urgency, PU# request before verification **Response:** "Great timing. Let me verify your carrier profile first. MC number?"

Scenario 2: The Familiar Stranger

> *"We've hauled for you guys before — pretty sure it was out of Chicago. Just need the shipper address for this one and we're good."*

Red flags: Claimed familiarity, address request **Response:** "Let me check our records. What's your MC number?"

Scenario 3: The Curious Dispatcher

> *"Quick question — is this electronics or general freight? We need to know for our insurance."*

Red flags: Commodity probing **Response:** "General freight. Standard cargo coverage applies. Ready to proceed with verification?"

Scenario 4: The Channel Switcher

> *"Can you just text me the details? Our email is down and I'm on the road."*

Red flags: Channel switch request **Response:** "We send all load details through official email. What's your company email address?"

The Information Cannot Be Unshared

Once any detail about a load is shared — weight, lane, commodity, dock contact, pickup window, equipment requirements — that information is permanent. It cannot be recalled. It cannot be qualified later. It enters the working knowledge of whoever picked up the phone.

This is the structural reality fraudsters exploit. **The caller you spoke with today does not have to be the carrier who steals the load.** They have to be the first call in a chain that may unfold over weeks.

- A caller who says "not interested" still walks away with whatever was shared before that point. The "not interested" is part of the technique — it ends the call before you ask harder verification questions.
- Fraudsters assemble fragments across multiple brokers — a commodity from one, a dock contact from another, a pickup window from a third, an equipment requirement from a fourth — until they have enough to impersonate, intercept, or redirect.
- By the time the actual fraud occurs, the trail to any single disclosure is invisible. The broker who overshared three months ago will never be linked to the loss.

Treat every unverified interaction as if you are speaking to the next theft. You may be. Not in the next hour. Possibly in the next week. The information you shared today is what makes that theft possible.

The protection is not in qualifying disclosure after the fact ("just between us," "off the record," "this stays here"). Once spoken, it does not stay. The protection is in disclosure discipline before the conversation begins — knowing exactly what stays withheld until carrier verification is complete, regardless of how the conversation goes, regardless of how the caller frames their reason for asking, regardless of whether they seem to walk away.

The information cannot be unshared.

Quick Reference Card

Print this. Keep it visible.

NEVER Share Before Verification:

- PU# / Pickup number
- Shipper address
- Consignee name/address
- Commodity type
- Dock contact names
- Rate confirmation

Red Flag Patterns:

- Urgency + info request
- Claimed familiarity + resistance to verify
- Multiple commodity questions
- Consignee questions before commitment
- Name fishing
- Channel switch requests

Safe Response:

> *"Let me verify your carrier profile. What's your MC number?"*

If They Push Back:

> *"This is our standard process. Once verified, we can move quickly."*

If Something Feels Wrong:

Log it. Report it. Trust your instincts.

Document Control

Version	Date	Author	Changes
1.0	May 2026	Y. Melnik	D74 Technologies whitepaper publication

These phrases are part of a broader social engineering protection framework. Use as a live reference during any dispatcher or carrier interaction.

SECTION 3

SOP 3: Warehouse Release Protocol

Section 3 — SOP 3: Warehouse Release Protocol

Pre-Pickup Verification

D74 Technologies Whitepaper — Operational Methodology for Carrier Fraud Prevention
Prepared by Yevgeniy Melnik | May 2026

Purpose

Prevent freight release to unauthorized parties by establishing verification checkpoints at driver arrival, during loading, and before seal application. This is the **last line of defense** before freight leaves your control.

Why This Matters

Most cargo theft happens at pickup — not in transit. A fraudster who:

- Has the PU# and shipper address
- Arrives early with a truck displaying the "right" MC number
- Sounds confident and professional

...can walk away with your customer's freight. By the time you realize the real carrier never showed up, the load is gone.

The facility is the final gate. Everything you verified digitally (authority, insurance, tracking) means nothing if the wrong truck gets loaded.

When to Use This SOP

Execute these steps for **every pickup** — not just high-value or flagged loads. Fraudsters target routine shipments precisely because brokers let their guard down.

Critical moments:

- Before releasing PU# to carrier
- When driver arrives at facility
- During loading
- Before seal is applied

Phase 1: Pre-Release Gate (Before Sharing PU#)

Do NOT release the pickup number, consignee name, or load details until:

1.1 Driver Verification Call

Call the **driver directly** — not the dispatcher.

Why: Dispatchers can be part of deception. The driver is physically present (or not).

What to confirm:

- [ ] Driver is aware of the load and pickup location
- [ ] Driver can describe where they are (gate, yard, street)
- [ ] Background sounds match a facility environment (trucks, forklifts, gates)

Listen for red flags:

- Dead silence or indoor quiet (driver not at a facility)
- Overly scripted or rehearsed answers
- Hesitation on basic questions about their location
- Dispatcher insisting you can't speak to driver

1.2 Shipper Confirmation

Call your **shipper contact** (shipping clerk, dock supervisor, or known contact).

Ask:

- [ ] "Has a truck arrived for [Load/PO#]?"
- [ ] "Can you see the MC number or company name on the truck?"
- [ ] "Does the trailer number match what we provided?"

If shipper uses kiosk check-in or can't visually confirm:

- Request photo from driver (see 1.3)

1.3 Photo Verification

Request a photo from the driver showing:

- [ ] Truck door with MC number or company logo visible
- [ ] Facility building or dock doors in background
- [ ] Current timestamp (driver sends via text/email)

Compare against:

- Photos from carrier onboarding (if available)
- Expected MC number and equipment

Red flags:

- MC number doesn't match (magnet decals can be swapped)
- Truck appearance differs from onboarding photos
- Background doesn't match shipper facility

1.4 GPS/Tracking Verification

Confirm tracking shows driver **at the shipper location**.

Recommended threshold: Driver should be within **0.1 miles** of facility.

Why this tight threshold:

- Industrial parks can have 10+ facilities in 0.2 miles
- "Close enough" GPS can mean wrong dock or staged impostor
- Fraudsters know brokers accept approximate locations

Red flags:

- GPS shows driver elsewhere while claiming to be on-site
- Tracking signal jumps or shows inconsistent movement
- Driver claims arrival but tracking hasn't updated

1.5 Release Decision

Release PU# and load details ONLY when:

Checkpoint	Status
Driver call confirms real-time presence	☐
Shipper confirms truck on-site (or photo received)	☐
MC/equipment matches expected carrier	☐
GPS shows driver at facility (≤0.1 mi)	☐

If ANY checkpoint fails: Hold release. Escalate to supervisor. Do not proceed until resolved.

Phase 2: Loading Monitoring

Once the driver is cleared and loading begins, maintain awareness until the seal is applied.

2.1 Periodic Check-Ins

During the loading window:

- [ ] Check in with driver: "Still at the same dock?"
- [ ] Confirm dock number hasn't changed
- [ ] Watch for unusual delays or driver going silent

Why: Trailer swaps and driver substitutions can happen during dock wait times.

2.2 Tracking Behavior

Monitor tracking for:

- [ ] Truck remains stationary at facility
- [ ] No unexpected movement before loading confirmed
- [ ] Tracking status changes match driver's verbal updates

Warning: Auto-tracking systems may mark load as "complete" based on time or geofence — this does NOT replace verbal confirmation from driver.

2.3 Hold Point Before Sealing

Before the seal is applied, confirm:

- [ ] Driver confirms freight is loaded
- [ ] Trailer number matches (no swap during loading)
- [ ] Driver has not received seal yet

Phase 3: Seal Verification

3.1 Seal Requirements

Two requirements operate **independently** — both must be met. Strength rating without dual-door binding is insufficient. Dual-door binding without strength rating is insufficient.

Requirement 1 — Dual-Door Binding (the seal design)

The seal must be a **long wired cable seal** (also called a *through-handle cable seal*) — a cable long enough to thread through *both* trailer door handles and lock back on itself, binding the two doors together as a single sealed unit.

Why this matters: Trailer doors close in sequence — the left door first, the right door closing over it — so a single-door seal on the right does physically constrain access. The vulnerability is not the door geometry. It is the seal itself. Most seals — including many

ISO-certified models — can be removed cleanly in under five minutes with no tamper evidence left behind. Once the seal is defeated, both doors open and the loss is not detected until delivery, by which point the trail is gone.

A long cable seal threaded through both door handles changes the calculation. The cable sits under tension wrapped around two handles; defeating it cleanly requires more time, more deliberate effort, and more visible activity at the trailer. It also signals — to dock workers, insiders, and any observer — that the carrier treats freight security as operational discipline rather than checkbox compliance. The friction and the signal are the protection.

Excluded (do not satisfy Requirement 1, regardless of strength rating):

- Bolt seals applied to a single door
- Short cable seals threaded through one handle
- Plastic indicative seals (zip ties, plastic snap seals)
- Any seal configuration that does not bind both door handles under tension

Requirement 2 — Strength Rating (the seal certification)

The seal itself must meet a defined strength standard.

Tier	Standard	Use case
Minimum	Steel cable seal, unique serial number, seal number recorded on BOL	Standard freight
High-value / regulated freight	**ISO 17712:2013 H-certified** (high-security) — meets pull, shear, bend, and impact resistance tests	Pharma, electronics, alcohol, hazmat, defense logistics, any load over carrier insurance threshold

Note on ISO 17712: The standard governs seal *strength* only. It does not require dual-door binding. A 17712-H bolt seal is compliant under the strength standard but does not satisfy Requirement 1. The two requirements must be evaluated independently when selecting a seal.

3.2 Seal Documentation

Request photo showing:

- [ ] Seal in place
- [ ] Seal serial number clearly visible and legible
- [ ] Cable **visibly threads through both door handles** (the cable should be photographable crossing between the two handles)
- [ ] Cable is **taut** between handles, not slack — a loose cable defeats the tension that makes the seal harder to defeat

Record:

- Seal serial number on rate confirmation and internal tracking
- Time seal was applied
- Who applied the seal (shipper, guard, clerk, or driver)
- Seal type and ISO 17712 rating if applicable

3.3 Seal Verification at Delivery

Instruct consignee to verify:

- Seal serial number matches BOL
- Seal is intact (not cut, spliced, or re-tied)
- Cable still binds both door handles as documented in the pickup photo
- Report any discrepancy immediately — do not allow unloading to proceed until verified

---

Red Flags Summary

Signal	Concern Level
Dispatcher won't let you speak to driver	High
Driver call has no background facility noise *	High
GPS shows different location than driver claims	High
MC number on truck doesn't match carrier file	Critical
Shipper can't confirm truck on-site	Medium
Tracking shows movement before loading confirmed	High
Seal applied before you confirmed load	High
Seal number doesn't match at delivery	Critical

*** On background noise as a signal:** Modern noise-canceling headphones can make a real call from a real facility sound nearly silent. Absence of background noise is a signal, not proof. When this red flag fires together with others and uncertainty remains, use the verification technique below.

Verification Technique — When Uncertainty Remains

If multiple red flags are firing but the driver is reportedly already at the shipper, and the call's authenticity is unclear: **ask the driver to hand the phone to the facility's shipping/receiving department.**

Why this works. A real driver at a real facility can physically walk to the shipping office and pass the phone to a clerk. The clerk picks up; you speak to them directly; you confirm the truck and driver are on-site. The hand-off itself is the proof — no actor or script can fake it remotely.

A scammer running the call from off-site cannot comply with this request. They cannot produce a real shipping clerk on demand. Watch for these evasions:

- "He's busy, I'll have him call you back" (the call back will not happen)
- "There's nobody available right now" (improbable during operating hours)
- "The driver just stepped out — I'll have him call you" (test by waiting; ask for the clerk directly)
- Sudden dropped call, static, or "bad signal"
- Argument that the request is unusual or unreasonable

When to use this technique:

- Cumulative red flags where driver is reportedly on-site but doubt persists
- Background noise is suspiciously absent despite claimed facility presence
- GPS and the driver's verbal location have a gap you cannot resolve
- Dispatcher has resisted other verification steps
- The load is high-value or in a known-risk lane

What this technique resolves: the physical impossibility for a scammer creates the discriminator. One short request, one short conversation with a shipper clerk, and the ambiguity collapses into a clear answer — either the driver is there, or the call was never genuine.

If the hand-off fails or is refused: treat as confirmation of fraud. Hold the load immediately. Move to escalation.

Escalation

Escalate immediately if:

- Multiple red flags in same pickup
- MC number mismatch confirmed
- Driver or dispatcher becomes evasive when questioned
- Shipper reports different truck than expected
- Seal discrepancy at delivery

Escalation path — freight still at the shipper (pre-pickup):

1. Hold the load (do not release PU#, addresses, or rate confirmation)
2. Notify operations lead / supervisor
3. Document everything (screenshots, call logs, photos, communication records)
4. Instruct the shipper to refuse pickup — if a truck arrives claiming to be your carrier, do not load
5. Report the attempt to industry channels: **TIA Watchdog**, **Highway**, and **FMCSA** if MC mismatch is confirmed
6. If a legitimate carrier's MC was being impersonated, notify that carrier directly so they can monitor for further misuse of their identity
7. Re-issue the load through a fully re-verified carrier; treat the original transaction as compromised

Escalation path — freight has already left the shipper (post-pickup):

The pickup-gate window has closed. The situation has shifted from prevention to recovery.

Switch to SOP 1 — First 48 Hours: Incident Response Playbook (Section 1 of this whitepaper) and engage that workflow immediately. The first 48 hours are critical for recovery; do not delay.

Quick Reference Checklist

Print this. Use for every pickup.

Before Releasing PU#:

- [ ] Called driver directly (not dispatcher)
- [ ] Driver confirmed location with real-time details
- [ ] Shipper confirmed truck on-site OR driver photo received
- [ ] MC/equipment matches expected carrier
- [ ] GPS shows driver at facility (≤0.1 mi)

During Loading:

- [ ] Checked in with driver during load window
- [ ] Tracking shows truck stationary at dock
- [ ] No unexpected movement or status changes

Before Seal:

- [ ] Driver confirmed freight loaded
- [ ] Trailer number still matches
- [ ] Seal number recorded
- [ ] Seal photo received (number visible, proper placement)

For Delivery:

- [ ] Consignee instructed to verify seal number
- [ ] Seal match confirmed at delivery
- [ ] Any discrepancy reported immediately

Document Control

Version	Date	Author	Changes
1.0	May 2026	Y. Melnik	D74 Technologies whitepaper publication

This checklist provides a framework for pickup verification. Implementation details may vary by organization, shipper relationships, and cargo type.

SECTION 4

Primer A: AVP — Human-Layer Deception Detection

Section 4 — Primer A: AVP — Human-Layer Deception Detection

D74 Technologies Whitepaper — Operational Methodology for Carrier Fraud Prevention

Excerpt from the Zero Trust Freight Security Framework © D74 Technologies
Prepared by Yevgeniy Melnik | May 2026

Purpose

Tools detect what's already happened. People detect what's about to happen.

AVP — Ask, Validate, Probe — is a conversation method that lets a carrier rep, dispatcher, or risk manager surface deception in real time. Without aggression. Without slowing legitimate carriers down.

It applies anywhere a human is on the other end of the line: pre-booking dispatcher calls, driver identity verification at pickup, in-transit check-ins, and delivery confirmation.

The Formula

Ask

Open with a real-time, open-ended question. Not yes/no. Not multiple choice. Something only a person physically present can answer immediately.

> *"Where are you staged right now?" "What exit just passed?" "Which dock did they assign you to?"*

Validate

Cross-check the answer against observable data the moment it arrives:

- GPS / ELD ping
- Phone tracking location
- Seal photo timestamp
- Prior call notes
- The driver's known schedule and equipment

If the answer hesitates, vagues out, or contradicts the data — that's the signal. Don't argue. Note it.

Probe

Rephrase the answer slightly to test for logic and recall.

> ***Rep:*** *"Where are you staged?"* ***Driver:*** *"I'm at Love's in Toledo."* ***Rep:*** *"Got it — Love's in Toledo. How's traffic over there right now?"*

A real driver answers naturally. A staged actor reading a script may stall, repeat the phrase verbatim, or pivot to a generic answer.

The probe isn't an interrogation tactic — it's a logic check disguised as conversation.

Why AVP Matters

Detection tools fire alerts after a pattern is established. AVP fires *while* the conversation is happening — before the freight is released, before the driver leaves the lot, before the deception locks in.

In red-team exercises we've run against broker teams, a substantial majority disclosed sensitive load information when asked the right way. The same teams would have been positioned to catch the impostor if they'd used AVP. The method costs nothing — it only requires that reps know how to use it.

When to Use AVP

AVP applies across multiple stages of the load lifecycle:

Stage	What AVP catches
Pre-booking dispatcher call	Impersonation, scripted responses, MC mismatch, identity inconsistencies
Pre-pickup driver call	Driver substitution, equipment mismatch, location spoofing
In-transit check-in	GPS spoofing, dispatcher deception, behavioral drift mid-trip
Delivery / POD review	Forged receipts, multi-tenant dock confusion, after-hours irregularities

It also extends beyond the carrier conversation:

Counterparty	AVP target
Shipper rep on a verification callback	Are they actually at the facility?
Receiver dock contact	Did the truck that arrived match the booking?
Insurance verifier	Is the policy genuinely active, or just printed PDF?

Failure Modes

Reps who don't understand the method end up:

- **Interrogating every driver equally**, including trusted carriers — burns relationships, generates alert fatigue
- **Asking vague or leading questions** disconnected from observable data — produces noise without signal
- **Confusing "thoroughness" with productivity** — wastes time on obviously low-risk carriers

AVP is a precision instrument, not a hammer. Used correctly, it speeds vetting up. Used incorrectly, it slows everything down.

AVP With Anchors — The Discipline

Don't probe randomly. Every probe must anchor to a real signal.

Valid anchors:

- A missed tracking ping
- A location mismatch between GPS and the driver's verbal report
- A prior behavioral oddity (rushed responses, scripted language, evasive answers)
- A seal concern (photo refusal, mismatched seal number)
- A documentation gap (delayed COI, mismatched W-9, MC age)

Example anchored probe:

> *"Tracking hasn't updated for the past 40 minutes near Miami — can you walk me through where you are and what happened earlier today?"*

This framing is collaborative, not accusatory. A real driver explains. A fraudster scrambles.

Without an anchor, AVP becomes interrogation — and reps lose the relationship even when no fraud was present.

Cultural Framing

Reps who feel rude using AVP usually conflate conversation with politeness. AVP is professional, not adversarial. The framing that works:

> *"It's not rude — it's policy. Every load. Every driver."*

Legitimate carriers expect this. Fraudsters do not. Carriers who push back on basic verification are themselves a signal.

How AVP Integrates with Escalation

AVP is a method, not a checklist. The output of an AVP exchange feeds into whatever escalation framework the broker already operates:

- A clean exchange (real-time answers, GPS-confirmed, anchored to verifiable data) resolves the concern and proceeds; log it for audit trail
- An ambiguous exchange (hesitation, contradiction, deflection without clear failure) gets logged and escalated for supervisor review
- A failed exchange holds the load pending further verification
- Repeated AVP failures from the same carrier across multiple loads are a structural signal — not a one-off

Each broker operates a different escalation framework — some quantitative (red-flag scoring with weighted thresholds), some qualitative (concern tiers like low/moderate/high), some procedural (named decision-makers at each escalation level). AVP outputs work within any of them. This primer covers the conversational method only; the escalation framework, the scoring calibration, and the decision authority are organization-specific and should be set by the operator based on load volume, lanes, and risk tolerance.

Training Application

For team training, AVP can be drilled in 15-minute role-play sessions:

1. **Trainer** plays dispatcher or driver
2. **Trainee** runs an AVP exchange against the call
3. **Trainer** switches between honest and deceptive answers between calls
4. **Group review** identifies which questions surfaced signal, which produced noise

Two or three sessions a quarter is enough to build muscle memory. The goal isn't to script the questions — it's to internalize the rhythm so reps improvise naturally when something feels off.

What AVP Does Not Do

AVP is not a replacement for:

- FMCSA / Highway / RMIS compliance checks
- Insurance verification
- Seal protocols
- GPS / ELD monitoring
- Identity document verification

It is the human layer on top of these systems. Tools handle the binary checks (active / not active, match / mismatch). AVP handles what no tool can: real-time judgment about whether the human on the other end is who they claim to be.

The two work together. Neither replaces the other.

SECTION 5

Primer B: Detecting Sold MCs Through Behavioral Drift

Section 5 — Primer B: Detecting Sold MCs Through Behavioral Drift

D74 Technologies Whitepaper — Operational Methodology for Carrier Fraud Prevention

Excerpt from the Zero Trust Freight Security Framework © D74 Technologies
Prepared by Yevgeniy Melnik | May 2026

The Problem

Sold MCs are the hardest fraud to detect because the entity is legitimate.

- The MC# matches FMCSA records
- Insurance is current
- Authority is active
- Years of clean compliance history make the carrier look like exactly what brokers want

Then the operation changes hands. The new operators inherit the credentials, the relationships, the booking history. They're inside the trust loop before anyone notices.

By the time a compromised load surfaces, the damage is already distributed across multiple shipments.

Banking-trail analysis catches some of this — payment patterns shift when ownership changes. But banking data is downstream. The behavioral data is upstream and immediately observable.

This primer covers six behavioral drift patterns that surface a compromised MC before the first fraudulent load completes.

Terminology note: "sold MC," "compromised MC," and "trusted carrier drift" are used interchangeably throughout this primer. They refer to the same phenomenon — a legitimate MC whose operations have changed hands or been quietly subverted, while the credentials, history, and trust signals remain unchanged on the surface.

Six Signals of Trusted Carrier Drift

1. Corridor Deviation

Every legitimate carrier has a known operating geography. Some are national. Most are regional — East Coast corridor, Midwest hub-and-spoke, Texas triangle, Florida–Northeast.

When a known-corridor carrier suddenly books loads *outside* their pattern — especially light freight, low pallet counts, or unusually high-margin lanes — investigate before booking.

Ask:

- Are they cherry-picking only the easiest loads?
- Are these one-offs or the start of a new pattern?
- Did these loads carry other red flags?

The wider a carrier's coverage area, the harder it is to verify shipper relationships and operational consistency. Fraudsters prefer tight corridors where they can repeat patterns without scrutiny. A sudden expansion is a signal, not a sales opportunity.

2. Capacity Mismatch

Every trucking operation has a realistic load-output ceiling driven by its operating model. The two main baselines:

- **OTR (Over-the-Road / long-haul):** A 10-truck fleet at reasonable utilization moves roughly **18–22 loads per week** — accounting for transit time, rest periods, dwell, and HOS compliance.
- **Local / regional:** A 10-truck local fleet running 1–3 loads per day per truck moves **50–180 loads per week**, depending on lane length, turn time, and dock dwell.

The fraud signal is not a fixed number — it is a **ratio**. When a carrier consistently moves **2–3× the load volume its fleet size and operating model can realistically support**, the carrier is one of:

- Misrepresenting fleet size
- Re-brokering quietly
- Consolidating without authorization
- Operating sub-carriers off the books

All four scenarios expose freight to uninsured risk. None of them stay clean for long.

Capacity audits should be quarterly minimum, with random sampling of carriers in the 70th+ percentile of load volume **within their operating-model peer group** — OTR fleets compared against OTR fleets, local against local. Cross-model comparison produces false positives in either direction.

3. SOP Awareness and Spoofing Alignment

The most sophisticated compromised carriers study your detection process and operate to stay inside it — learning roughly where your thresholds sit and shaping their behavior to look consistently, unnaturally compliant.

This is the hardest pattern to detect because the carrier *looks compliant*. The signal is the absence of any signal — operational hygiene that is too consistent to be organic. Real operations are messy. A carrier whose record is *flawless* across a long run of loads — nothing that ever trips a review — can warrant the same scrutiny as one with visible red flags. A record with no friction at all can mean a counterparty managing to your process rather than simply running freight.

Keep the specific signatures that separate "managed-to-look-clean" from "genuinely clean" calibrated to your own operation and held internally. A detection threshold written down where a counterparty can read it is one they can learn to operate beneath.

4. Receiver-Level Exploitation

A compromised carrier studies *your receivers*' SOPs as carefully as they study yours.

- They know which large national DCs accept box trucks even when the original booking specified a 53-ft dry van
- They know which receivers process loads too quickly to verify the trailer matches the booking
- They know which loading docks have visibility gaps

The freight gets delivered. The receiver signs. The substitution stays invisible — until a downstream incident traces back through the chain.

5. The Trust Loop

This is the structural reason sold MCs are hard to catch:

- The better they perform, the more they're trusted
- The more trust they have, the more control they gain
- More control means more freight, fewer red flags, more immunity
- More immunity means longer runways before exposure

The longer this loops, the more catastrophic the eventual exposure. A trusted-carrier failure rarely produces one bad load. It produces months of compromised handoffs that surface as a cluster.

6. Tech Behavior Forensics

Modern compromised MCs leave digital traces:

- Overlapping IP addresses across multiple MCs
- Domains linked to multiple carrier identities
- Spoofed email headers
- A "trusted carrier" opening a second account under the same phone number, address, or owner name

Cross-MC infrastructure overlap rarely happens by accident.

Behavioral Clues — Summary

Clue	What It Suggests
Load volume far exceeds fleet size	Re-brokering or capacity misrepresentation
Tracking refusals outside known corridor	Unauthorized sub-carrier use
Driver or trailer information reuse across loads	Equipment misrepresentation
A record too flawless to be organic (no friction across many loads)	SOP awareness, possible spoofing
Tracking or handoffs clustering after-hours	Reduced staff monitoring — a known fraud window
Cross-MC infrastructure overlap (IPs, domains, contacts)	Same operator running multiple identities

Real-World Risk

This isn't just about margins. Compromised carriers have been documented to:

- Add counterfeit or altered goods mid-transit
- Re-broker to unvetted carriers (substitution, contamination, unauthorized consolidation)
- Transport sensitive freight (pharmaceuticals, food, electronics) under a trusted MC banner while routing it through unverified hands

Case example. A trusted carrier hauled a load of flour — same shipper, same commodity they'd handled dozens of times. This time they re-brokered mid-transit. What traveled with the flour during the handoff? Nobody knows. The receiver may have flagged a shortage. The carrier absorbed it quietly.

The real risk wasn't the financial loss. It was that the flour now traveled with unknown freight — possibly including hazmat — through a chain no auditor could later reconstruct. That's not a margin event. That's a recall event, a contamination event, and in regulated commodities, a criminal liability event.

Countermeasures

These don't require new technology. They require operational discipline:

- **Monitor regional lanes** — flag outlier activity outside the carrier's normal corridor
- **Audit load volume vs. stated fleet capacity** — quarterly, at minimum
- **Audit tracking gaps by lane and time of day** — identify after-hours patterns
- **Randomize photo confirmation requirements** — truck, trailer, seal, every N loads, unpredictable timing
- **Audit historical load assignments** — surface hidden driver or equipment overlap across MCs
- **Re-verify trusted carriers every 90 days** — even if every prior load was clean
- **Treat each carrier like an extension of your operations team** — know their lanes, their drivers, their equipment, their why

The "trusted carrier" designation is not permanent. It's a rolling 90-day window — at minimum, and preferably more often.

Know Your Carriers Like Your Team

Carrier reps must treat their carriers like an extension of their own operations:

- **Where do they run?** East Coast only? Midwest corridor? If they suddenly book from Washington to Florida, that's a flag.
- **Who drives for them?** Recognize driver names and voices. Consistency matters.
- **What equipment do they own?** If they claim a new truck, ask for proof (registration, photo, COI).
- **Why are they deviating?** Every off-pattern move needs a valid explanation. "Just helping a buddy" isn't good enough.

If a carrier typically runs FL–IL but suddenly books a load from WA, you flag it. That's not paranoia. That's due diligence.

Why This Matters Now

Sold MCs are widely identified across the freight industry as one of the highest-priority unsolved problems in carrier fraud. FMCSA's Motus system (live as of May 2026) introduces identity and business verification at the registration layer, but the existing carrier base benefits only as those entities cycle through re-verification. Until that propagates, behavioral pattern detection is the only practical defense brokers have.

These signals don't require new vendor tools. They require organized observation, audit discipline, and a willingness to question a relationship that's been clean for years.

The data patterns don't lie. The question is whether your operation is looking at them.

SECTION 6

Related Industry Resources

Section 6 — Related Industry Resources

How this whitepaper sits alongside existing industry guidance

D74 Technologies Whitepaper — Operational Methodology for Carrier Fraud Prevention
Prepared by Yevgeniy Melnik | May 2026

Where This Whitepaper Sits

This whitepaper documents operational methodology — what to do, specifically, at the points where freight fraud most often succeeds. Several industry and government resources address adjacent layers of the same problem. A working broker should have visibility into all of them.

Resource	Layer it covers	Access
TIA Framework to Combat Fraud (April 2024)	Industry-wide awareness, fraud taxonomy, case studies, member resource network	TIA member resource library
FBI IC3 — ic3.gov	Federal cargo theft reporting; case routing for interstate theft and high-value cargo	Public
FMCSA NCCDB — nccdb.fmcsa.dot.gov	Formal complaint channel for motor carrier authority violations and identity misuse	Public
FMCSA Motus (May 2026 rollout)	Identity and business verification at the motor carrier registration layer	Public
Verisk / CargoNet industry data	Theft trend data by commodity, location, day of week, lane	Subscription / partner channels

The methodology in this whitepaper is designed to work alongside these resources, not to replace any of them. The awareness, taxonomy, and reporting infrastructure provided by TIA, FBI, FMCSA, and the major insurance and data partners is the context this whitepaper assumes the reader already has access to or knows how to find.

This whitepaper extends that context into the operational layer: scripts, methods, and decision frameworks for the moment of carrier interaction.

D74 Technologies offers this whitepaper as a supplemental operational resource. The TIA Framework to Combat Fraud and the federal resources cited above remain authoritative within their respective scopes.