



## Freight University Study Guide

### Chameleon Carriers, Double Brokering, Identity Hijacking & Audit Fraud — The LFS-AOS Way

Companion to the video/audio session: *Freight Fraud and Chameleon Trucking Companies Study Session*

#### Lesson Objective

By the end of this study guide, you will be able to:

- Explain how the modern freight fraud ecosystem works in **2-0-2-6**.
- Identify the **4 threat families** and their shared weakness.
- Run the **Four Gate Freight Fraud Firewall** on every load.
- Apply **Rate Con Ready** before you sign.
- Build a **fraud-proof load file** that survives disputes.
- Execute the **Response Ladder**: Detect → Document → Escalate → Educate → Prevent.

#### The Big Idea

**Fraud is defeated by structure.** Your protection is not software. It's a repeatable operating doctrine built into your company.

#### How to Use This Guide

- Read the guide once straight through.
- Then run the **Exercises + Homework** with your real operation.
- Print the **Checklists** and keep them at dispatch.

#### Visual Timeline (12 Subject Images)

Use 1 image per subject during playback.

1. **The Architecture of Deception**
2. **The 9-7% Target Problem**
3. **Chameleon Carriers: Identity Recycling**
4. **Verification Modernization (ARCHI logic → Motus reality concept)**
5. **Double Brokering: The Silent Theft**
6. **Cyber-Enabled Fraud: Hijacking, BEC, Voice Spoofing**
7. **Government Impersonation & Audit Fraud**
8. **Cargo Theft: Hotspots & Commodity Targeting**
9. **LFS-AOS Doctrine: System, Not Software**
10. **The Four Gate Freight Fraud Firewall**
11. **Document Security = Payment Security**
12. **Response Ladder: Detect → Document → Escalate → Educate → Prevent**

## **Core Concepts (What You're Learning)**

### **1) The Architecture of Deception**

**What it is:** Fraud is organized, data-driven, and systematic. It's not "random bad luck."

**Reality check:** Fraud thrives where operations are fast, pressured, and inconsistent.

#### **Example (the load that never pays):**

- POD signed, rate con looks clean
- Broker claims payment was sent
- Factoring says paperwork invalid
- Phone disconnects, email disappears

- Fraudster “reborn” under a new identity

**Key takeaway:** If your process depends on trust, you are vulnerable.

## 2) The 9-7% Target Problem

**Why small carriers get hit first:**

- Spot market reliance
- Fast onboarding
- Cashflow pressure
- Factoring dependency

**One-Hit Insolvency Factor (your business chain reaction):**

Unpaid load → cash gap → fuel/maintenance stress → insurance risk → payroll stress → authority instability.

**Self-audit question:** If you lost 1 load payment this week, how many weeks until your operation is in emergency mode?

## 3) Chameleon Carriers (Identity Recycling)

**Definition:** A carrier that shuts down one authority and reappears under another to escape claims, enforcement, debt, or history.

**How they survive:** They change identity, but they recycle infrastructure.

**Chameleon Red Flags (Continuity Signals)**

- Shared **phone numbers** across multiple entities
- Shared **addresses** (suites, mail drops, virtual offices)
- Same dispatch behavior across “different” companies
- Recycled emails with small spelling changes
- Insurance cycles that look unstable (start/stop patterns)
- Equipment continuity that “moves” between entities too neatly

**Example:** “New authority” with a story that claims scale, but no operational footprint to match.

**Rule:** You don’t accuse. You **flag risk**, then verify.

#### **4) The Battlefield: 4 Threat Families (1 shared DNA)**

**The 4 threat families:**

1. **Chameleon carriers**
2. **Double brokering fraud**
3. **Identity impersonation & credential hijacking**
4. **Government impersonation / D-O-T / F-M-C-S-A audit fraud**

**The shared DNA:** They rely on you **accepting identity without proving it**.

**The pressure point:** Speed + urgency + inconsistent process.

#### **5) Double Brokering: The Silent Theft**

**Fraud version (simple lifecycle):**

1. Fraudster poses as a carrier to accept load
2. Reposts load pretending to be a broker
3. Real carrier hauls freight
4. Fraudster collects paperwork
5. Fraudster gets paid
6. Real carrier is left unpaid

**Why it’s deadly:** Chain of custody breaks → disputes rise → insurance denial risk increases.

**Example:** “Send the POD to this different email” mid-load or post-delivery.

## 6) Cyber-Enabled Fraud (Credential Hijacking, BEC, Voice Spoofing)

**What changed:** Criminal groups now attack the channels.

### **Common tactics:**

- Stolen load board/FMCSA credentials
- Look-alike emails and domains
- Business Email Compromise (bank routing swaps)
- Voice spoofing for reroute scams

**Rule:** Assume the channel can be compromised. Verify identity **independent** of the channel.

**Mid-load rule:** No reroute, no address change, no receiver change without verification through the original verified contact.

## 7) Government Impersonation & Audit Fraud

**The trap:** Scammers impersonate authority to steal EINs, logins, banking, or charge fake fees.

### **Red flags:**

- Non-.gov domains
- Urgent payment pressure
- Requests for sensitive info via unsolicited email/phone
- Payment requests through peer-to-peer apps

**Rule:** Verify through official numbers you pull yourself, not through their link.

## 8) Cargo Theft: Hotspots & Commodity Targeting

**Modern reality:** Criminals study lanes and target high-resale commodities.

### **Think like an investigator:**

- Where is the freight easy to steal?

- What commodity resells fast?
- What lanes are “repeatable” targets?

**Your job:** Run lane intelligence before criminals run it on you.

## **The LFS-AOS Doctrine (This is the system)**

### **9) LFS-AOS is not software**

It’s an internal operating doctrine: structure before movement.

#### **Circular Integrity Model:**

**Detect → Document → Escalate → Educate → Prevent**

**Why it matters:** When 1 carrier is defrauded, insurance rises. Costs rise. Margins shrink. Vulnerability grows. The cycle feeds itself.

## **The Two Critical Operating Systems**

### **10) The Four Gate Freight Fraud Firewall**

**No load moves until all 4 gates pass.**

#### **Gate 1: Identity**

- Who are you really?
- Call-back protocol using independently sourced numbers
- Match dispatcher name/role to entity

#### **Gate 2: Authority**

- Does the authority profile match the story?
- New authority risk handling
- Footprint logic: stability and operational shadow

#### **Gate 3: Insurance**

- Verify insurance directly (not forwarded PDFs)
- Confirm active policy, dates, and insured entity match

## **Gate 4: Documents**

- Rate con integrity (version control)
- Pickup/delivery instruction provenance
- Bank change verification protocol
- POD chain control

**Pass/Fail rule:** If any gate fails, you do not “negotiate.” You treat it as a risk outcome.

## **11) Rate Con Ready (Pre-booking routine)**

**Doctrine:** The moment before you sign is not paperwork time. It’s decision time.

**Rate confirmation is not a paycheck. It’s a risk contract.**

### **Rate Con Ready checklist**

- Independently verify the counterparty
- Confirm authority
- Confirm insurance
- Confirm documents (rate con version integrity)
- Confirm payment terms (who pays, when, how)

**Rule:** Verify first. Then move.

## **12) Document Security = Payment Security**

If you want to win disputes, you build certainty.

### **Your Fraud-Proof Load File (minimum standard)**

- Signed rate confirmation (final version)
- Email thread screenshots + headers when possible
- Call log: who called, what number, when

- Insurance verification proof
- Pickup evidence: photos, timestamps, BOL, seal numbers
- Delivery evidence: POD photos, GPS/time-stamped proof, receiver name
- Invoice packet: consistent, clean, chronological

**Driver doctrine:** The driver is an evidence deliverer.

## **Response Ladder (When something feels wrong)**

**Detect → Document → Escalate → Educate → Prevent**

### **Step 1: Detect**

- Identify anomalies (identity mismatch, reroute pressure, document swaps)

### **Step 2: Document**

- Freeze the timeline: screenshots, call logs, versions, POD evidence

### **Step 3: Escalate**

- Notify the correct parties (shipper/broker/factor) using verified contacts
- File reports through appropriate channels as required by your operation

### **Step 4: Educate**

- Turn the incident into a training example inside your company

### **Step 5: Prevent**

- Patch the process: update your Four Gate checks and Rate Con Ready routine

## **Student Tools (Copy/Paste Checklists)**

### **A) 60-Second Red Flag Scan**

- Too urgent, too fast, too pushy
- Email domain mismatch or slight misspelling
- “Send documents to a different email”
- Bank details change midstream
- Refusal to verify identity by call-back
- Story doesn’t match footprint

## **B) The “No Exceptions” Rules**

- No load without Four Gate pass
- No reroute without verified approval
- No bank change without verified call-back
- No POD sent to unknown addresses

## **Practice Scenarios (Do these with your team)**

### **Scenario 1: Chameleon Carrier Continuity**

You’re offered a load by a carrier/broker. Everything looks new and polished.

- What continuity signals do you check first?
- What triggers a risk flag?
- What is your pass/fail decision?

### **Scenario 2: Double Broker Loop**

You tender a load. A “dispatcher” asks for POD to be sent to a different email.

- Which gate is failing?
- What evidence do you preserve?
- Who do you call back—and how?

### **Scenario 3: Mid-Load Reroute**

Driver receives a call: “Receiver changed. New address now.”

- What is the protocol?
- What is the exact verification path?

#### **Scenario 4: Audit Scam**

You receive an “urgent compliance notice” demanding sensitive info.

- What are the red flags?
- What do you do instead?

#### **Homework (Real-World Assignments)**

##### **Homework 1 — Build Your Four Gate SOP (1 page)**

Create a one-page SOP your dispatcher can run every time.

- Include pass/fail criteria
- Include call-back protocol
- Include what documents must be saved

##### **Homework 2 — Build Your Rate Con Ready Template**

Create a repeatable template:

- Counterparty verification log
- Authority check notes
- Insurance verification proof
- Payment terms confirmation

##### **Homework 3 — Create Your Fraud-Proof Load File Folder**

Set up a digital folder structure:

- 01 Rate Con
- 02 Authority
- 03 Insurance

- 04 Pickup Evidence
- 05 Delivery Evidence
- 06 Invoice & Payment
- 07 Communications (Email/Call logs)

#### **Homework 4 — Run 10 Load Audits**

Pick 10 past loads (or 10 future opportunities).

For each one:

- Could you prove identity?
  - Could you prove authority?
  - Could you prove insurance verification?
  - Could you prove chain-of-custody?
- Score each gate pass/fail.

#### **Homework 5 — Team Drill (30 minutes)**

Run Scenario 3 (reroute scam) as a live roleplay.

- Dispatcher script
- Driver script
- Verification call-back script

#### **Self-Test (Quick Knowledge Check)**

Answer in writing:

1. What is the shared DNA across the 4 threat families?
2. Why is a rate confirmation a risk contract?
3. Name the 4 gates and 1 pass/fail rule for each.
4. What evidence must exist in a fraud-proof load file?
5. What is the Response Ladder in order?

## **Where This Lesson Fits (Study Plan Logic)**

**Curriculum fit:** Scam Prevention & Verification + Dispatch Systems + Compliance Intelligence.

### **Prerequisites (recommended):**

- Basic broker/carrier onboarding fundamentals
- Dispatch workflow basics

### **Recommended next lessons:**

- Credit-First Dispatch Discipline (payment protection)
- Carrier/Broker Onboarding SOP Mastery
- The Freight Research Engine (lane intelligence + counterparty intelligence)

## **Final Reminder**

You are not protected by your intentions. You are protected by your systems.

**Verify or fail.**