HIGHWAY

# Freight Fraud Index Report

# Q4 2025

Inside the Shift from Impersonation to Legitimate Theft

Freight Fraud Index

# Executive Summary

2025 marked a clear inflection point in freight fraud. By year-end, **direct thefts accounted for nearly half of all reported stolen loads**, surpassing compromised inboxes and manipulated ownership changes as the leading drivers of loss. Unlike prior years, these incidents were increasingly carried out by carriers with legitimate operating histories, real equipment and deep familiarity with broker and shipper workflows — signaling a shift from impersonation-based fraud to the exploitation of trusted access.

At the same time, compromised email remains a high-impact attack path, with fraudulent email attempts rising **117% year-over-year,** alongside continued abuse of stolen MCs. Across all vectors, Highway data shows a consistent pattern: fraud succeeds when identity is assumed rather than continuously verified.

The message for 2026 is straightforward: **Trust must be validated at every stage of the load lifecycle**. Brokers who enforce identity-first workflows, verify the full contact chain, and act quickly on risk signals significantly reduce exposure. As fraud moves deeper into legitimate operations, discipline — not complexity — remains the most effective defense.

2025 In Review

# Fraud Patterns, Pressure, and the Rise of Identity Risk

In 2025, freight fraud didn’t escalate because controls failed, it escalated because assumptions went unchallenged. As market pressure, regulatory scrutiny, and operational strain intensified, fraud increasingly emerged from inside otherwise legitimate operations, exploiting gaps between onboarding, booking, and execution. The result was a year defined not by louder attacks, but by quieter failures of verification.

**Three patterns defined 2025:** Direct thefts rose to the leading fraud vector, driven by legitimate carriers executing calculated, multi-load events. Compromised inboxes remained a high-impact access point despite declining volume. Change of ownership, or “sold MCs”, continued to provide quiet entry into broker networks.

Year-Over-Year Comparison

# The State of Freight Fraud

## Fraudulent email attempts

▲ 117%

**914,719** in 2024 vs **1,986,995** in 2025

## Unauthorized FMCSA contact changes

▼ 99.1%

**109,672** in 2024 vs **958** in 2025

## Identity alerts reported

▼ 23.9%

**11,992** in 2024 vs **9,129** in 2025

## Top countries

| | |
|---|---|
| 2024 | Mexico \| Pakistan \| India |
| 2025 | Serbia \| India \| Lithuania |

**UNDERSTANDING THESE METRICS**

The numbers in this snapshot represent threats that Highway detected and blocked before they could disrupt operations.

Together, these metrics show more than just volume — they reveal patterns, hot spots, and the value of proactive, identity-first fraud prevention. They provide brokers with actionable insights to verify, monitor, and respond to threats before shipments or payments are compromised.

# 2025 Freight Fraud Trends

**5,581**

**Carrier users from 71 countries**

attempted to log into Highway from outside of North America and failed.

**Top countries**

Serbia | India | Lithuania

**1,986,995**

**Fraudulent inbound emails blocked**

**958**

**Unauthorized FMCSA contact changes**

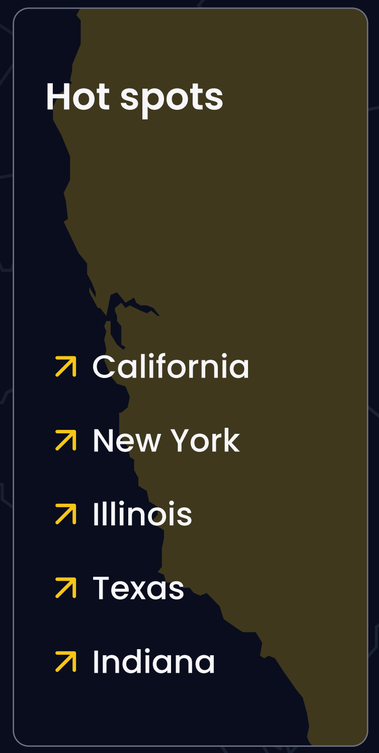
**8,525,962**

**Fraudulent and spoofed phone calls blocked**

**9,129**

**Fraud-related identity alerts reported**

**Hot spots**



- California
- New York
- Illinois
- Texas
- Indiana

**Top targeted commodities** Food & Beverage | Electronics | Cosmetics

Based on Highway App, Inc. data from January - December 2025

Top 2025 Fraud Vectors

# When Trust Becomes the Threat

1

# Direct Theft by Rogue Carriers

Direct thefts emerged as the leading freight fraud vector in Q4 2025. Highway observed a consistent pattern of incidents frequently carried out by carriers with legitimate operating history, real equipment, verified VINs, and expected appointment details. In many cases, changing visa, licensing, or regulatory pressures caused these carriers to “break bad,” triggering a deliberate shift in behavior. Using their knowledge of routes, shipper workflows, receiver behavior, and broker relationships, the fraudsters used their own trucks to move multiple loads quickly and delay detection.

# Why Now?

Highway's Risk team identified a measurable increase in direct theft incidents coinciding with heightened regulatory and licensing scrutiny, particularly related to **non-domiciled commercial driver licensing**. As federal and state scrutiny intensifies, some carriers viewed their ability to legally haul freight as time-limited, increasing the likelihood of sudden, high-risk behavior from previously compliant operators.

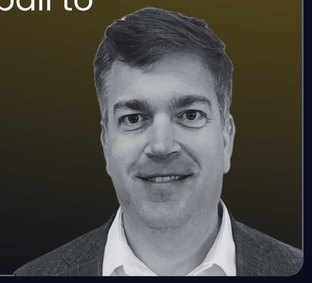
Public audit findings reinforce this trend. A recent article from Transport Topics found that **more than 25% of non-domiciled CDLs in California** were improperly issued, including licenses that remained valid beyond the holders' authorized stay. In response, the state announced plans to revoke approximately 17,000 improperly issued CDLs. At the federal level, regulators have warned that states failing to align with Federal Motor Carrier Safety Administration (FMCSA) licensing standards may face withheld highway funding.

From a risk perspective, this regulatory tightening introduces instability into parts of the carrier population. In multiple Q4 investigations, Highway observed carriers with long delivery histories and previously clean records executing direct thefts shortly before license expiration, revocation, or anticipated enforcement action.

These incidents were not opportunistic — they were calculated, multi-load events carried out by drivers and fleets with deep operational familiarity.

As enforcement activity accelerates into 2026, Highway is closely monitoring the regulatory-driven risk signals that are expected to play a larger role in freight theft patterns. Brokers using Highway have the ability to limit access to carriers with flagged or non-domicile statuses, reducing exposure to high-risk drivers.

> "Direct theft is the hardest to combat because these carriers were once trusted. There's no crystal ball to predict when someone with a clean history is going to break bad."
>
> MICHAEL GRACE
> VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY



# Common Patterns

- Small changes to driver, dispatcher, or FMCSA contacts before theft
- Hot spots in California and other states with non-domiciled licensing issues
- High-value loads targeted: food & beverage, electronics, copper, protein powder, cosmetics
- Multiple thefts executed quickly by familiar carriers
- Theft timed near license expirations or enforcement actions
- Fraudsters using legitimate MCs, insurance, and equipment

# Best Practices

- **Don’t ignore signals.** If a driver phone, email, or dispatcher name has been flagged before, pause and re-verify — even if everything else looks normal
- **Verify the full contact chain on every high-risk load.** Driver phone, dispatcher email, VIN/plate, and any last-minute changes must match known records.
- **Report theft as soon as it happens.** Timely reporting is the difference between a single incident and a multi-load theft run.
- **Trust with caution.** Past reliability doesn’t eliminate today’s risk.

---

**Highway customers reduce exposure by using identity checks and alert history to validate who is authorized to act — not just which MC is on paper.**

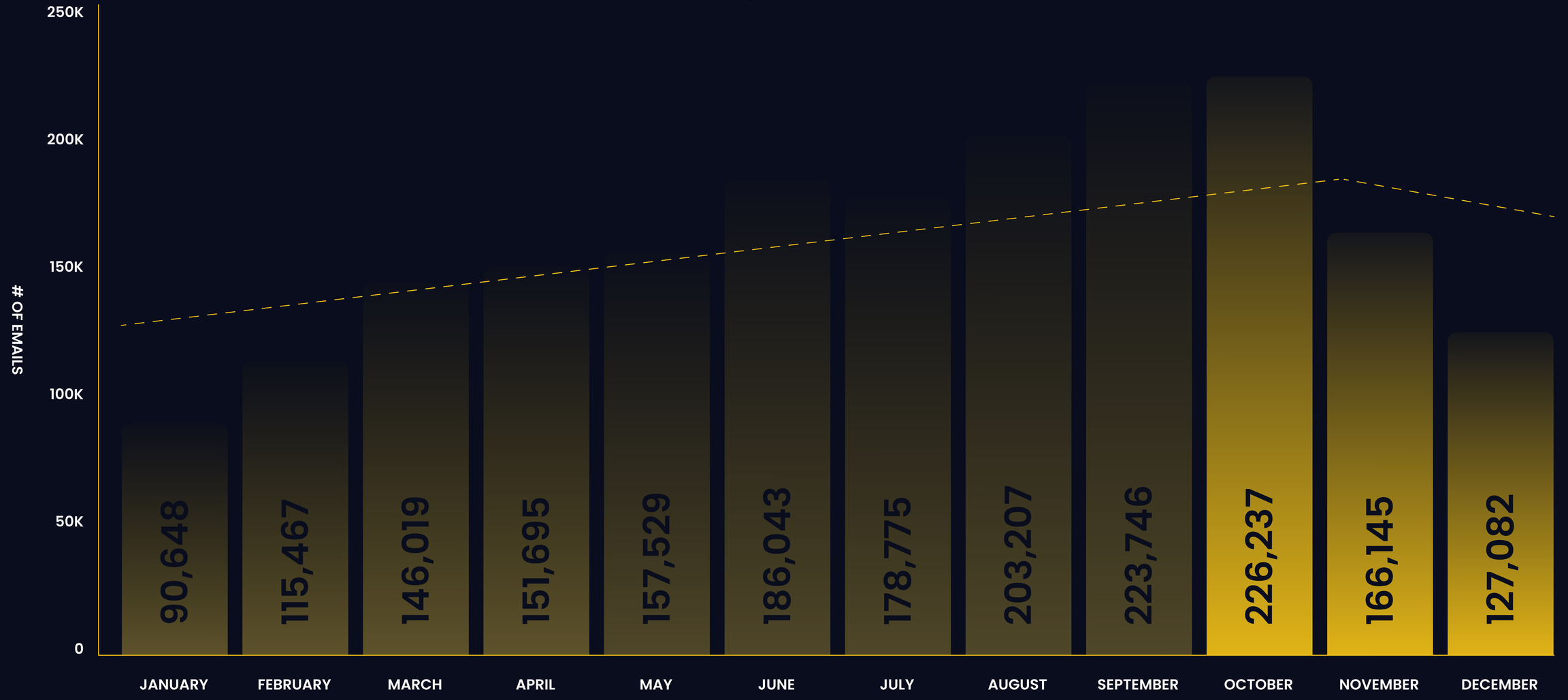
# 2 Compromised Inboxes

Even as direct theft rose to the top in Q4, compromised email has remained one of the most dangerous attack paths because it provides immediate access to high-value information: load details, pickup numbers, routing, rate confirmations, and payment instructions. Highway blocked 1,986,995 fraudulent email attempts in 2025, up by 117% from the 914,719 attempts recorded in 2024.

**Why it works:**
Once fraudsters have access to broker or carrier inboxes, they can impersonate trusted parties to reroute shipments or redirect payments. Although the frequency of email-based attacks has decreased relative to direct thefts, they remain a **high-risk** vector that requires vigilance and robust verification processes for teams.

# Fraudulent Emails Blocked by Highway

January-December 2025



Q4 2025 Trend

# How to Build Your Email Defenses

Effective email defense starts with verifying who is actually communicating, not just trusting what appears in the inbox. Identity-based controls, such as Highway's Carrier Identity Engine, combined with alerts and continuous monitoring help identify fraudulent emails and prevent them from influencing load decisions, payment instructions, or routing changes.

As email threats continue to evolve, maintaining secure, identity-first communication practices remains critical to protecting your freight, preserving trust between brokers and carriers, and reducing financial risk.

## Best Practices

- Require secure delivery workflows for rate confirmations and sensitive documents
- Enforce MFA and access controls across dispatch and carrier sales inboxes
- Confirm routing/payment changes with an outbound call to verified contacts
- Treat "reply-chain familiarity" as a risk factor — not proof of legitimacy

"Secure rate delivery has made a real difference. As adoption increases, we're seeing fewer email-based thefts."

MICHAEL GRACE
VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

3

# Sold MCs & Ownership Changes

Manipulated ownership changes, often labeled as “Sold MC” activity, continues to be one of the most consistent entry points for fraud in the freight ecosystem. While earlier in the year, change of ownership activity accelerated, Q4 continued to show elevated alert volume across the Highway network.

These events occur when fraudsters acquire or take over a legitimate MC, and reuse the carrier’s established identity to book loads, reroute freight, or extract payments. On paper, everything appears valid: authority is active, insurance is in place, and historical broker relationships remain intact.

Rather than relying on surface-level credentials, Highway surfaces change of ownership risk through alerts when the contacts, communication patterns, or operational behavior associated with a carrier shift in ways historically tied to fraud.

Q4 2025 Trend

# Red Flags to Watch for

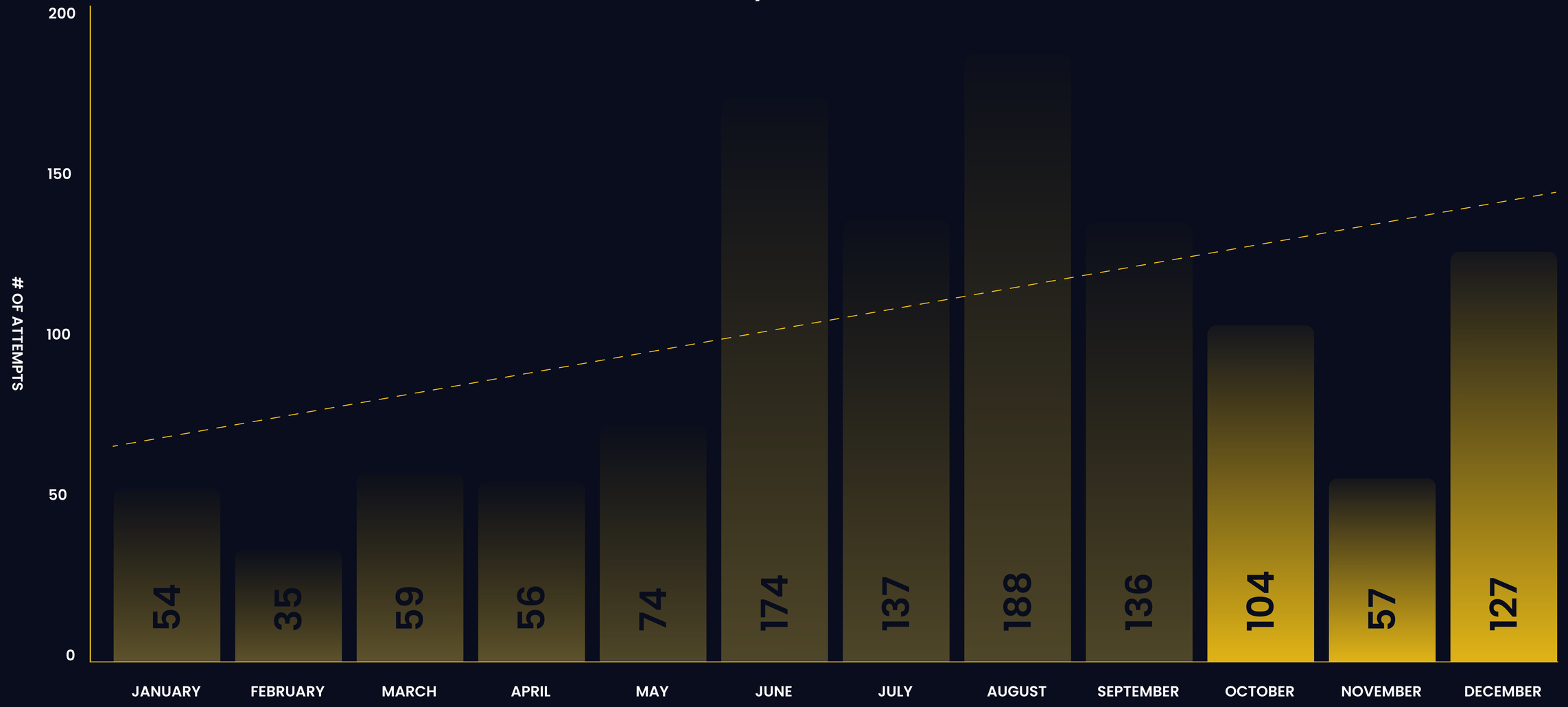
- A previously dormant carrier suddenly reactivates after several months of inactivity
- New emails, phone numbers, or users that conflict with the carrier's historical profile
- Behavioral changes that don't align with prior booking, communication, or dispatch patterns
- Reuse of contact information already associated with prior fraud events
- Access or activity patterns that don't align with how the carrier has historically operated
- Unusual urgency around payment changes, rerouting, or dispatch instructions

"In today's freight environment, trust can be transferred with a signature and an MC number. That's why brokers can't just verify companies anymore, they have to verify who is actually operating behind the authority."

MICHAEL GRACE | VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

# Change of Ownership Reports

January-December 2025



# Staying Ahead of Sold-MC Schemes

Timely reporting remains critical. When suspicious activity or theft events are reported through Highway, associated identities are immediately incorporated into the network's intelligence, enabling faster detection and suppression of future attempts.

In an environment where trust can be transferred as easily as an MC number, preventing sold MC fraud depends on continuously verifying who is actually operating behind the authority. Identity-first detection and shared intelligence remain one of the most effective ways to contain this threat and limit its impact across the industry.

**These indicators are surfaced as alerts within Highway workflows, allowing brokers to act without having to manually reconstruct ownership history.**

- Verify the person behind the MC, not just the company name. Identity-first checks reveal whether the user is authorized to act on the carrier's behalf.
- Cross-reference alerts with historical activity to spot sudden changes or inconsistencies.
- Encourage timely reporting of suspicious activity; the faster a potential theft is flagged, the sooner it can be investigated and mitigated.

Brokers who adopt layered approach to identity verification and proactive monitoring gain confidence that every carrier in their network is legitimately who they claim to be and authorized to act. In an ecosystem where trust is bought and sold, prioritizing Carrier Identity is now a fundamental line of defense.

Emerging Trend Going Into 2026

# Valid Pickup Driver Redirect

**Valid Pickup Driver Redirect** is an emerging fraud vector observed in late 2025 where a load is tendered to a legitimate carrier and picked up correctly, but is later compromised through a spoofed communication appearing to come from the broker and is sent to the driver or dispatcher.

In these cases, everything at pickup checks out — the correct carrier, truck, VIN, and pickup number. The fraud occurs **after the load is already in transit**. A bad actor sends an email or places a call that appears to come from the broker, using lookalike domains or spoofed contact information toggle. The message instructs the driver to reroute the shipment, often citing routine issues like lack of dock space, a receiver change, or an updated delivery location. These requests are frequently paired with additional pay to create urgency and legitimacy.

This vector succeeds by exploiting trust and familiarity. Because the carrier and pickup are valid, drivers are more likely to comply — sometimes delivering the freight to a fraudulent drop location before the broker realizes the load has been redirected.

# Red Flags to Watch For

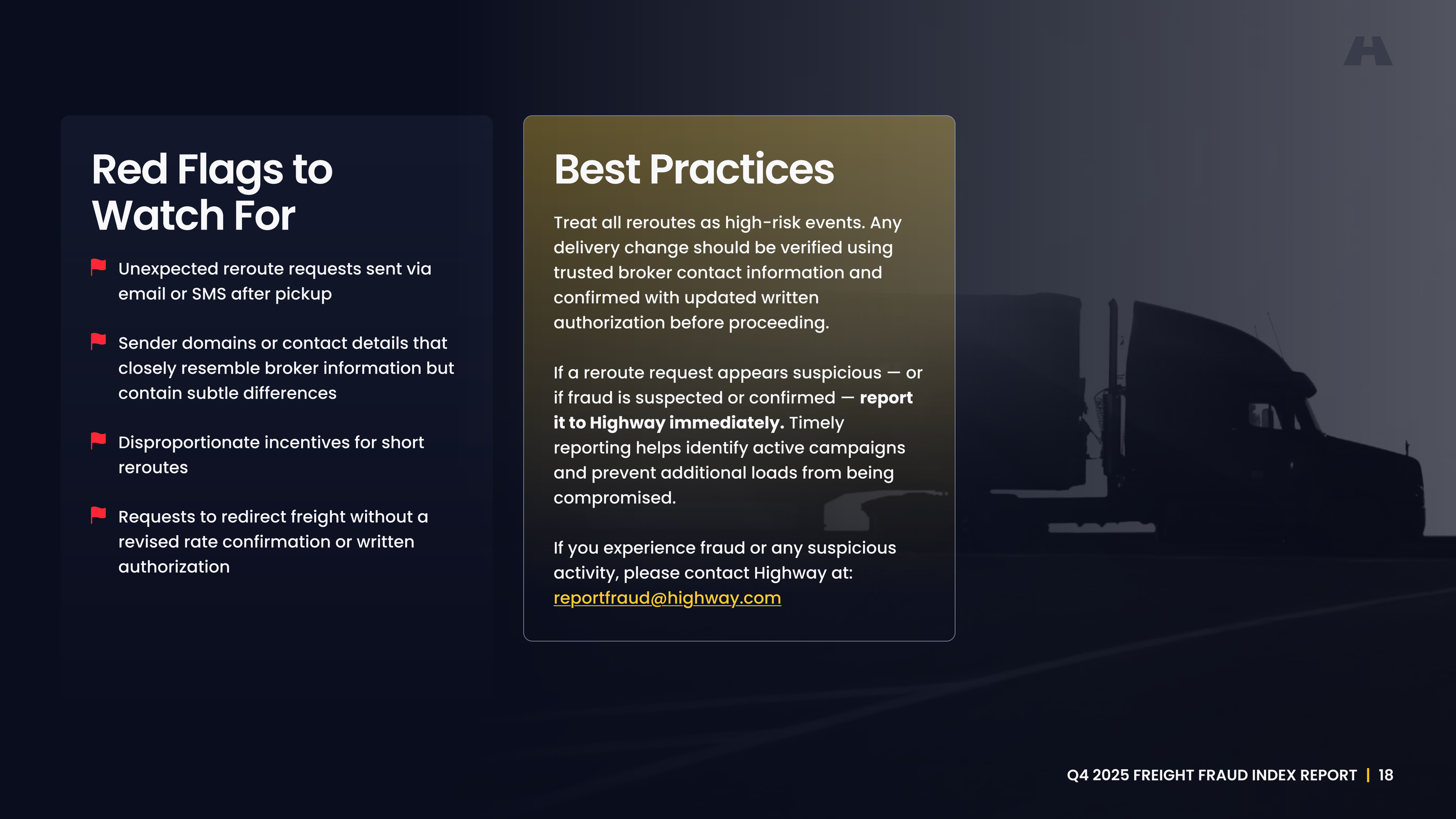
- Unexpected reroute requests sent via email or SMS after pickup
- Sender domains or contact details that closely resemble broker information but contain subtle differences
- Disproportionate incentives for short reroutes
- Requests to redirect freight without a revised rate confirmation or written authorization

# Best Practices

Treat all reroutes as high-risk events. Any delivery change should be verified using trusted broker contact information and confirmed with updated written authorization before proceeding.

If a reroute request appears suspicious — or if fraud is suspected or confirmed — **report it to Highway immediately.** Timely reporting helps identify active campaigns and prevent additional loads from being compromised.

If you experience fraud or any suspicious activity, please contact Highway at: reportfraud@highway.com



Identity-First Protection in Action

# Identity Is the New Battlefield

Today's fraud isn't happening in the shadows — it's happening out in the open.

Expiring visas prompting rogue behavior. Drivers exploiting equipment access. Bad actors steering pickups. Direct thefts traced back to legitimate carriers have gone bad. And compromised emails that look more convincing than ever.

In a landscape like this, information is the most powerful tool we have. The faster a bad actor is reported, the faster the next theft is prevented. The more shared, secure communications, across brokers and carriers, the safer every load becomes.

Highway exists to connect these signals, to give the industry a single place to verify, report, and act before fraud escalates.

**Protect Your Network Before the Next Threat Hits.**

Schedule a Demo ↗


highway.com