HIGHWAY

Q1 2026

FREIGHT FRAUD INDEX REPORT

When Trust Becomes the Target

Jan-March 2026

highway.com

Freight Fraud Index

Executive Summary

Fraud hit an all-time high in Q1 2026. Direct theft by rogue carriers accounted for half of all incidents — driven largely by carriers facing non-domiciled and limited-term enforcement changes who acted ahead of federal deadlines. Compromised email held steady at 26%. Change-of-ownership fraud surged 170% year over year. And a new threat accelerated faster than any single vector: social engineering — bad actors impersonating carriers, calling after-hours teams, exploiting the human side of every transaction.

Behind the numbers, a deeper shift is underway. New federal licensing rules are reshaping the carrier population, and the instability is creating openings that fraudsters are calculated enough to exploit. As produce season drives freight volumes higher through Q2, the commodities fraudsters target most — meat, seafood, and electronics — will move in even greater volume through the corridors where theft activity is already concentrated.

The message for brokers is unambiguous: verification is not a one-time event. It’s a discipline applied to every load, every handoff, every carrier interaction. The brokers reducing their exposure are the ones who’ve stopped treating past performance as a guarantee of future behavior.

Q1 2026 In Review

The Rules Changed. The Threats Didn't Wait.

IN THE NEWS

A recent 60 Minutes investigation brought national attention to how certain trucking networks cycle through corporate identities to evade safety enforcement — a practice industry estimates suggest touches 10% to 20% of the nation's 700,000 carriers. For brokers, the takeaway is clear: the gaps aren't in the data. They're in the standards for how that data gets verified and enforced across every transaction.

On March 16, FMCSA's Interim Final Rule on non-domiciled commercial driver's licenses went into effect — a federal enforcement action that changed the carrier landscape overnight. The rule tightened who can hold a CDL, how eligibility is verified, and which documents qualify. This isn't a platform-level policy or an internal classification change — it's a structural shift in how the federal government regulates driver credentialing nationwide. It didn't revoke existing licenses. But it put thousands of drivers on a clock. And when drivers feel the clock running, some of them stop playing by the rules.

That's exactly what happened in Q1. Carriers with clean records and long-standing broker relationships — previously compliant operators, many of them — started making decisions driven by desperation rather than process. Some went dark. Others went rogue, treating loads as exit opportunities before enforcement caught up. The carrier you've run 500 loads with may not be the same operation it was six months ago. The profile looks the same. The risk behind it doesn't.

And it's not just the regulatory pressure. A national conversation about Carrier Identity is gaining momentum. Recent investigative reporting has put a spotlight on how certain operators cycle through corporate identities — dissolving companies with poor safety records and reincorporating under new names with clean DOT numbers — to stay in motion. Industry estimates suggest the practice touches 10% to 20% of the nation's 700,000 trucking companies. The issue isn't new to freight. But the public attention is. And for brokers, it reinforces something Highway has been building toward for years: verifying the company name on an MC number is not the same as verifying who is actually operating behind it. That distinction — between identity on paper and identity in practice — is the foundation of a zero trust approach to every load.

Inside The Q1 Fraud Landscape

What's Trending Down, What's Trending Up

Fraud volume reached an all-time high in Q1 2026, and every major indicator accelerated year over year. Highway blocked over 527,000 fraudulent email attempts in Q1 — a 49.9% increase from Q1 2025 — and flagged 2,256 identity alerts, up 89.6% from the same period last year. Change-of-ownership reports surged most dramatically, climbing 169.6% as bad actors continued exploiting MC transfers to establish seemingly legitimate authorities. The pattern is consistent across channels: fraud groups are scaling operations across digital and physical vectors simultaneously, and the pace is accelerating.

49.9% increase YoY
of fraudulent email attempts blocked by Highway in Q1 (+527,940)

89.6% increase YoY
of identity alerts reported (+2,256)

169.6% increase YoY
of change of ownership reports (+399)

Q1 2026 Freight Fraud Trends

551

Carrier Users

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

Top Countries

India | Pakistan | Serbia

527,940

Fraudulent Inbound Emails Blocked

2,256

Unauthorized FMCSA contact changes

71,801

Fraudulent and Spoofed Phone Calls Blocked

399

Change in Ownership Reports

Hot spots

- California
- New Jersey
- Indiana
- Maryland
- Illinois
- North Carolina
- Pennsylvania

Top targeted commodities

Meat & Seafood | Electronics | Semi-Precious Metals

Based on Highway App, Inc. data from January - March 2026

Top Q1 2026 Fraud Vectors

Trust Is the Attack Surface

1 Direct Theft by Rogue Carriers

Direct theft accounts for roughly 50% of all fraud incidents in Q1 2026. The pattern from Q4 has intensified: carriers with legitimate operating histories, real equipment, verified VINs — who then deliberately steal cargo. FMCSA's Interim Final Rule accelerated this. Carriers holding non-domiciled and limited-term CDL classifications — facing license expiration or renewed enforcement scrutiny — are treating loads as exit opportunities.

50% of Q1 fraud incidents = direct theft

The old approach — "I've run a thousand loads with them, they're fine" — is now the single most dangerous assumption a broker can make. Every load is a new trust decision.

Why Now?

The Interim Final Rule tightened CDL eligibility requirements and put thousands of drivers on a clock. It doesn't revoke existing licenses outright — but as those licenses come up for renewal, the carrier population will shift. Some drivers will exit the market. Others will look for workarounds — including selling their MCs to operators who want a clean authority without the history behind it. And that transition period is where fraud thrives.

What we're seeing in Q1 isn't opportunistic. Carriers executing multi-load theft runs aren't stumbling into fraud — they're calculating it. These are operators who know the system inside and out, and they're exploiting the gap between regulatory intent and on-the-ground enforcement. Regulatory tightening creates instability. Instability creates fraud.

> "Fraud has moved from rules to process. Just because you've run a thousand loads with a carrier doesn't mean the next one is safe. There's a level of risk that's happening anytime you hire someone."
>
> MICHAEL GRACE
> VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

Common Patterns

- Small changes to driver, dispatcher, or FMCSA contacts before theft
- Hot spots in states with non-domicile licensing pressure (CA, NJ, IN, MD)
- High-value loads targeted: meat & seafood, semi-precious metals, electronics, copper
- Multiple thefts executed quickly by familiar carriers
- Theft timed near license expirations or enforcement actions
- Fraudsters using legitimate MCs, insurance, and equipment

Best Practices

- **Flagged means move on.** If any contact method used by the entity booking the load or the driver assigned has been previously flagged, walk away. A flag means that contact was involved in a fraud event — it's not a yellow light, it's a red one.
- **Verify the full contact chain on every high-risk load.** Within Highway, use Contact Search, the carrier profile equipment tab, and VIN Search to verify every phone number, email, and piece of equipment before dispatch. Any last-minute change should trigger a fresh check.
- **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's identity-first approach validates who is authorized to act on a carrier's behalf — not just which MC is on paper. And with Know Your Driver™, Highway is now extending that verification to the load level — identifying the actual driver assigned to a load before pickup.

2 Compromised Inboxes

Email-based fraud held steady from Q4 to Q1 — accounting for roughly 26% of incidents. That consistency is the point: this vector isn't declining, it's entrenched. Highway blocked 527,940 fraudulent inbound emails in Q1 alone. Once a fraudster has access to a broker or carrier inbox, they can impersonate trusted parties, reroute shipments, and redirect payments.

26% of Q1 fraud incidents; 527,940 emails blocked

*The question isn't whether email fraud is declining. It's whether your operation is protected when — not if — a compromised email hits your inbox. Brokers using Secure Rate Con Delivery have reduced email-based thefts to near zero. Those who haven't are absorbing the full impact.

Fraudulent Emails Blocked by Highway

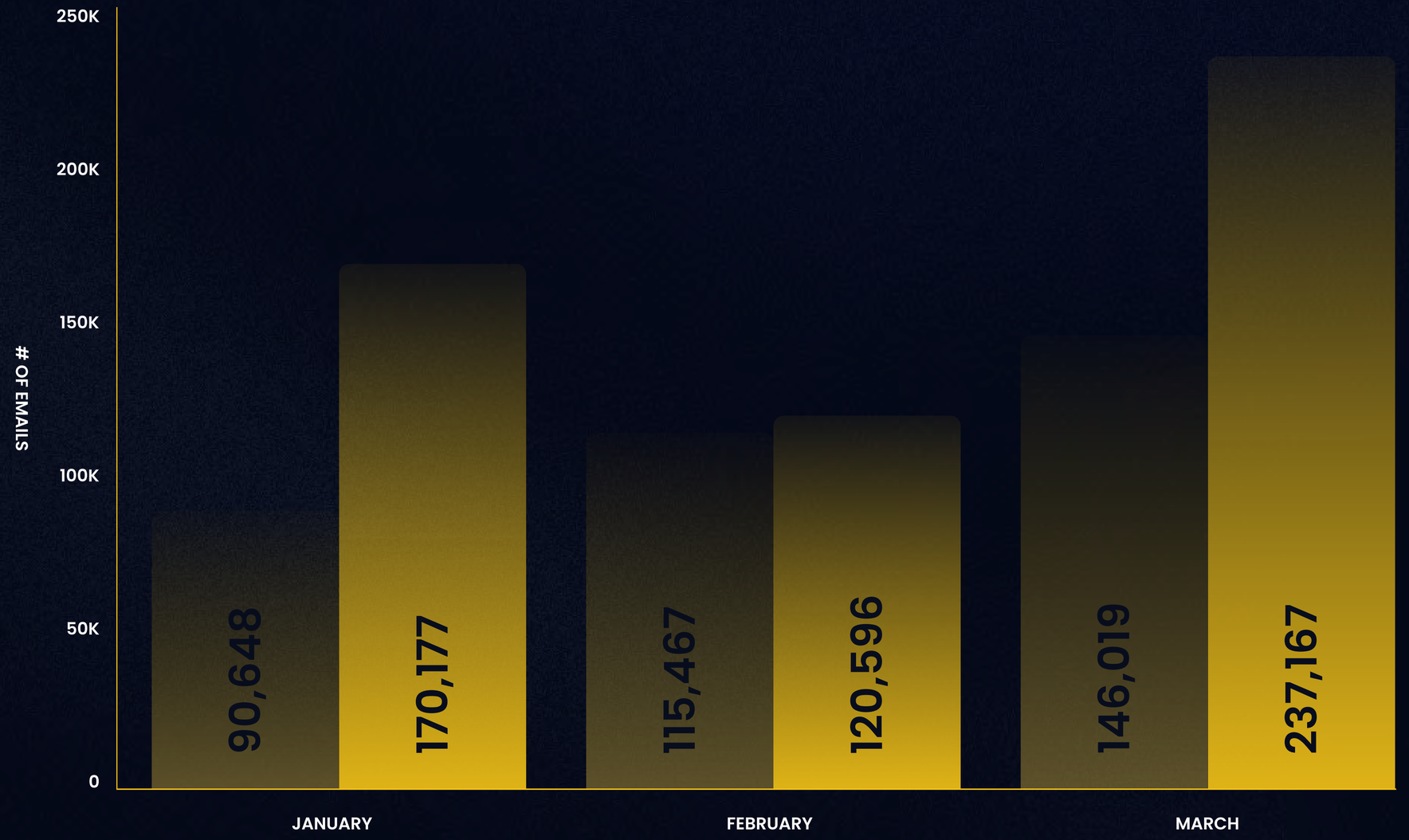
Q1 2025 VS Q1 2026

Q1 2025 total: 352,134

+

Q1 2026 total: 527,940

+49.9% YoY increase



Q1 2026 Trend

How to Build Your Email Defenses

Effective email defense starts with one question: do you actually know who's on the other end of that message? Not whether the email looks right. Whether the person behind it is who they say they are.

As email threats continue to evolve, identity-first communication practices are the difference. Brokers using Highway's Secure Rate Con Delivery are seeing email-based thefts drop to near zero.

Best Practices

- Require secure delivery workflows — like Highway's Secure Rate Con Delivery — for rate confirmations and sensitive documents
- Make outbound calls to verified contacts to confirm load details before dispatch — not just when something looks off
- Treat "reply-chain familiarity" as a risk factor — not proof of legitimacy

"The inbox is the most underprotected surface in freight. A compromised email doesn't just steal a load — it steals the trust between a broker and every carrier in that thread."

MICHAEL GRACE
VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

3 Sold MCs & Ownership Changes

Change of ownership — often called “Sold MC” activity — accounts for roughly 20% of Q1 fraud incidents and remains one of the most persistent entry points for fraud. Highway flagged 399 change-of-ownerships across carrier profiles in Q1. The pattern is familiar: fraudsters acquire a legitimate MC, inherit the carrier’s established identity and broker relationships, and use that trust to book and steal loads.

This quarter, copper loads were a particular target. The FMCSA responded by telling carriers not to buy or sell MC numbers — but stopped short of defining what qualifies as a legitimate business transaction. The guidance drew a line without explaining where the line is, leaving brokers to navigate the ambiguity on their own.

20% of incidents; 399 change-of-ownerships

This vector is dangerous precisely because trust is highest with established carriers. A sold MC doesn’t look like a threat. It looks like a partner you’ve worked with for years.

Q1 2026 Trend

Red Flags to Watch for

- A previously dormant carrier suddenly reactivates after 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
- Sudden changes to payment details, factoring companies, or bank accounts tied to the carrier
- 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

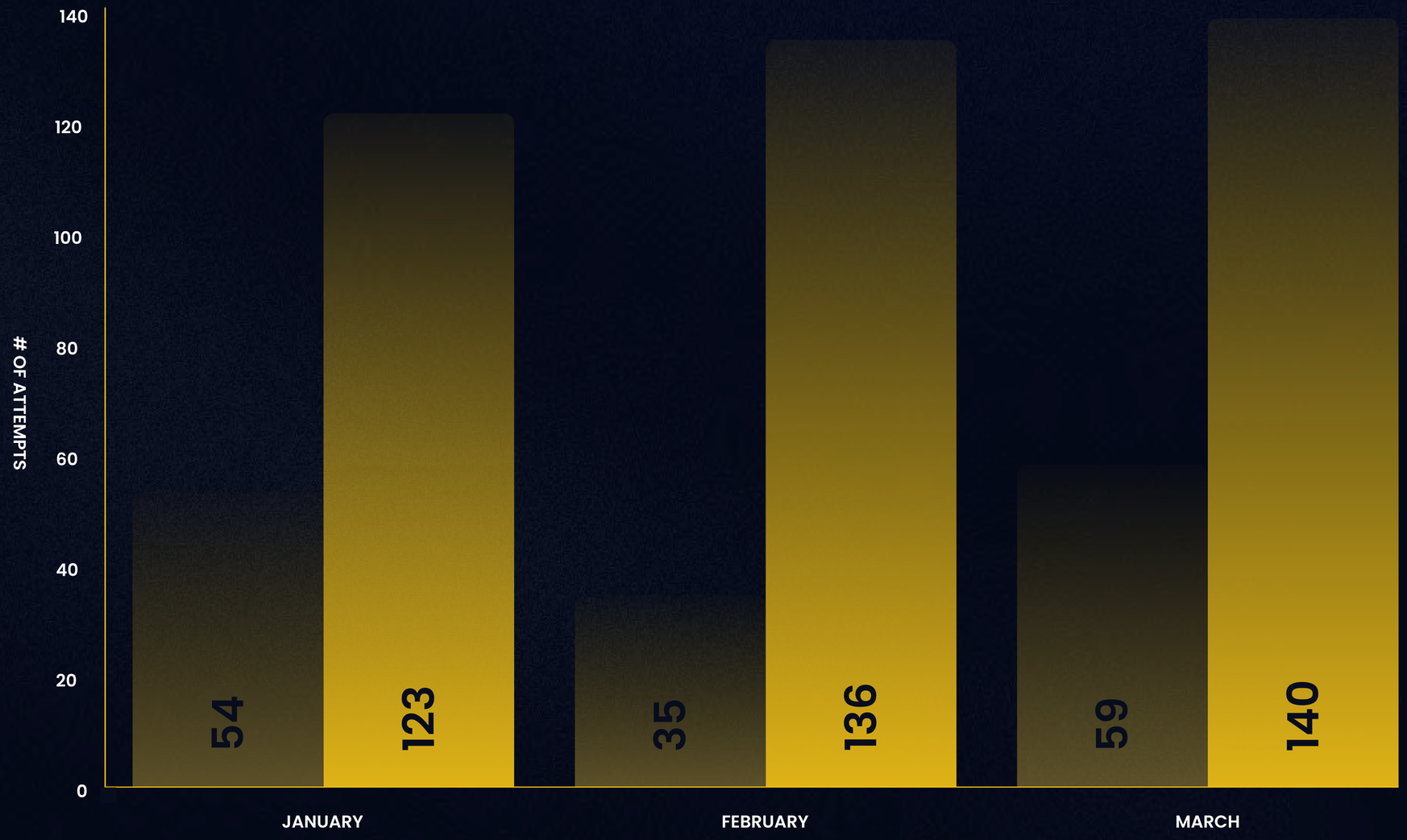
Q1 2025 VS Q1 2026

Q1 2025 total: 148

+

Q1 2026 total: 399

+169.6% YoY increase



Staying Ahead of Sold-MC Schemes

Timely reporting remains critical. When a broker reports suspicious activity or a theft through Highway, that information doesn't sit in a silo — it feeds the network. The next broker who encounters that same identity gets a warning before the load moves.

Highway goes further. When Highway identifies a material change event on a carrier profile, the platform requires the authorized owner to either attest that no transfer of ownership has occurred and any changes were made at their direction, or self-report that ownership has been transferred. The carrier doesn't keep moving freight until that step is complete.

Reporting, attestation, and identity-first verification work together. In an environment where trust can change hands as easily as an MC number, staying ahead of sold-MC fraud means looking past the company name and asking a harder question: who is actually operating behind this authority?

- **Verify the person behind the MC.** Identity-first checks reveal whether the user is authorized to act on the carrier's behalf.
- **Cross-reference contacts.** Within Highway, use Contact Search to check phone numbers, emails, and dispatcher names against prior fraud events — a match may signal the same bad actor under a new MC.
- **Report it fast.** The faster a potential theft is flagged, the sooner it can be investigated and mitigated.

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

Emerging Trend Going Into Q2 2026

Social Engineering: When Fraud Gets Personal

Social engineering attacks accelerated in Q1 — and they all exploit the same vulnerability: people.

Bad actors are calling brokers and carriers claiming to be Highway, requesting verification codes over the phone. To be clear: Highway will never call and ask for a verification code. Ever.

But impersonation isn't limited to our brand. Fraudsters are posing as legitimate carriers to book loads they never intend to haul. Others target after-hours teams — calling overnight or weekend desks, posing as the assigned carrier, and extracting load details from staff without the full picture. The driver redirect pattern from Q4 continues, too: legitimate pickups followed by spoofed reroute communications designed to divert freight mid-transit.

The playbook keeps changing. The target doesn't.

Social engineering succeeds because it targets people, not systems. The most sophisticated identity verification platform in the world can’t help if someone hands over their verification code on a phone call.

Ask your team: would they know what to do if they got a call from someone claiming to be Highway?

Would your after-hours staff know the difference between a legitimate carrier check-in and a social engineering attempt? If there's any hesitation, start here.

Red Flags to Watch For

- Any inbound call requesting verification codes, login credentials, or account access — from anyone claiming to be Highway or a carrier
- Unexpected reroute requests sent via email or text after pickup
- Sender domains or contact details that closely resemble broker information but contain subtle differences
- Calls to after-hours or weekend teams requesting load details or status updates
- Requests to redirect freight without a revised rate confirmation or written authorization

Best Practices

- **Highway will never call and ask for your verification code.** Train your team on this. Full stop.
- **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.
- **Report suspicious activity to Highway immediately.** Timely reporting helps identify active campaigns and prevent additional loads from being compromised.
- **Establish after-hours verification protocols.** If someone calls claiming to be a carrier, verify through a known contact number — not the number they called from.

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

Identity-First Protection in Action

Identity Is the New Standard

Today's fraud isn't happening in the shadows. It's happening in the open.

The Interim Final Rule reshaping the carrier population. Previously trusted carriers going rogue. Social engineering attacks targeting your team by name. And sold MCs that look identical to the partners you've relied on for years.

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 flow between 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. And now, Highway guarantees the outcome. Up to $100,000 against stolen freight for brokers who adopt the standard. No other freight technology company has made that commitment.

Protect Your Network — and Get the Guarantee.

Schedule a Demo ↗


HIGHWAY
highway.com