HIGHWAY

Freight Fraud Index Report Q3 2025

Fraud Trends You Can’t Afford to Ignore

Freight Fraud Index

Executive Summary

Q3 marked a significant shift in the pattern that has defined 2025: direct thefts have now surpassed compromised emails and ownership-change abuse as the leading drivers of fraud, with rogue carriers continuing to account for a significant share of direct theft and pilferage events. For brokers, carriers, and shippers, understanding these vectors and how to defend against them is critical.

The message this quarter is clear: prevention = back to the basics.

Highway data shows that organizations who consistently enforce the fundamentals of fraud prevention experience dramatically fewer fraud incidents, proving that discipline, not complexity, is the strongest defense in the freight industry.

Q3 2025 Freight Fraud Trends

762

carrier users from 40 countries

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

605,728

Fraudulent Inbound Emails Blocked

149

Unauthorized FMCSA Contact Changes

62,531

Fraudulent and Spoofed Phone Calls Blocked

2,992

Fraud-Related Identity Alerts Reported

Hot Spots

- California
- Texas
- Florida
- Indianapolis

Top Countries

India | Serbia | Pakistan

Top Commodities Targeted

Meat | Seafood | Electronics

Based on Highway App, Inc. data from July - September 2025

Inside The Q3 Fraud Trendline

What's Trending Down, What's Trending Up

Although total theft volumes trended slightly downward from Q2, the overall frequency and sophistication of attempted fraud continued to climb. Highway blocked over 605,000 fraudulent email attempts in Q3 (a 22% increase quarter over quarter) and 62,531 fraudulent phone numbers, a 47% quarterly increase. Broker-reported Identity Alerts also rose 31%, indicating not only stronger detection through Highway's network but also sustained pressure from fraud groups operating across digital and physical channels.

22% increase QoQ
of fraudulent email attempts blocked by Highway in Q3 (+605,000)

47% quarterly increase
of fraudulent phone numbers (+62,531)

31% quarterly increase
of broker-reported identity alerts (+2,992)

TOP Q3 FRAUD VECTORS

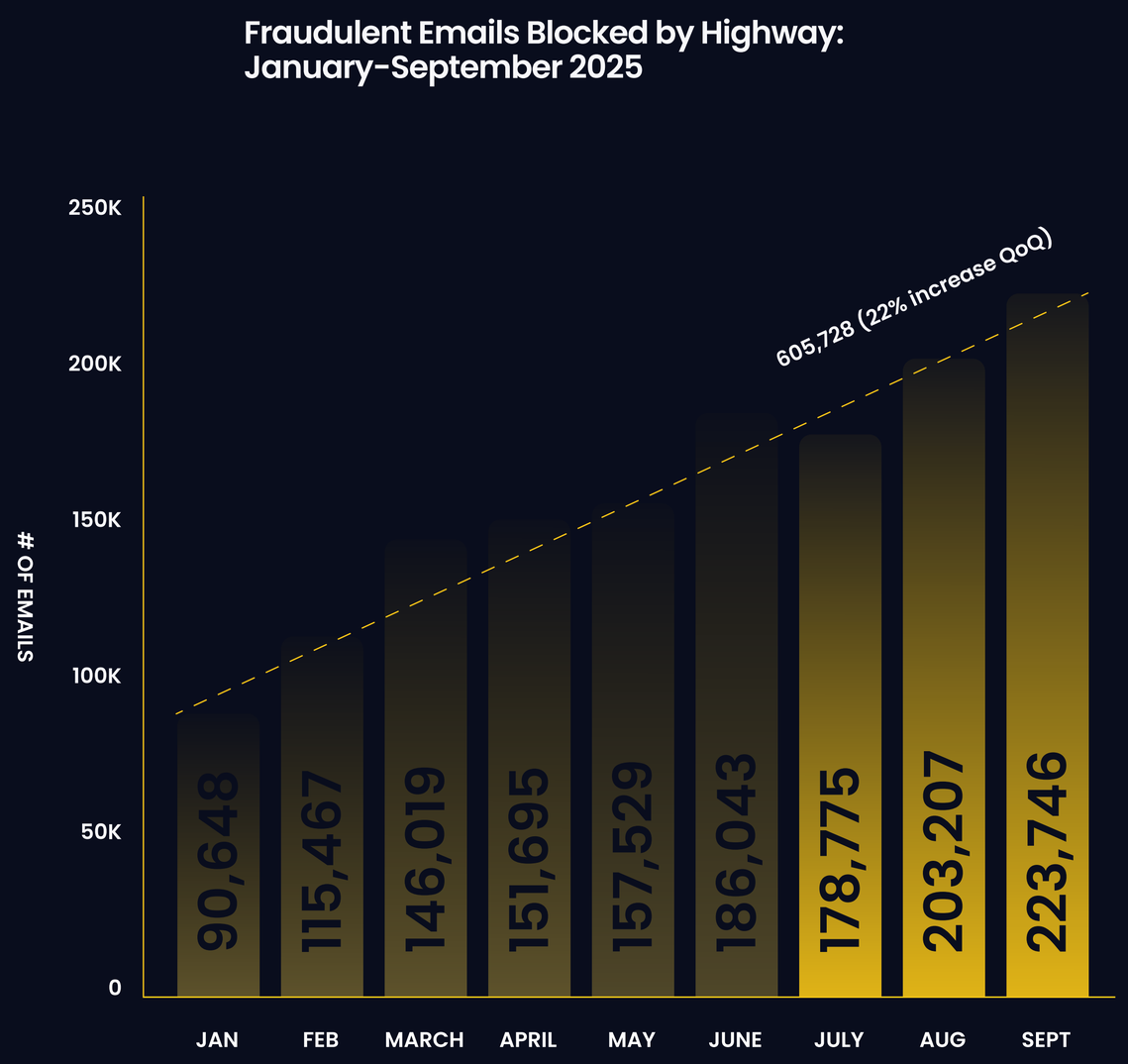
Shifting Patterns Powering Freight Fraud

1 Compromised Inboxes

Phishing and inbox takeovers remain the leading cause of freight fraud. In just the first nine months of 2025, Highway has already blocked 1,453,129 fraudulent email attempts—a 59% increase that surpasses the 914,719 attempts blocked during all of 2024.

Fraudsters continue to exploit broker and carrier emails because they are often the most vulnerable point of entry. It's the easiest way to gain access to sensitive information like load details and payment instructions that then can be used to impersonate legitimate carriers, reroute freight, or redirect payments.

Once inside an email thread, attackers blend seamlessly into ongoing conversations, sending authentic-looking updates that trick teams into trusting them.



Q3 2025 Trend

One Email Can Lose A Load

Imagine this: You're a broker sending a rate con to a carrier that you've used for months; but the carrier's email was hijacked that morning. The impersonator now has access to the emails you are sending. Once they come across a thread that includes a rate con, the bad actor replies and accepts the load, then immediately deleting the thread before the real carrier could notice. The load gets assigned and is never to be seen again.

Without proper verification, a single compromised email can trigger a chain reaction — from fake tenders to stolen freight. This is why Highway emphasizes secure communication practices and outbound verification as non-negotiable. Verifying the sender before booking, confirming rate cons through trusted channels like Highway's Secure Rate Confirmation Delivery, are critical steps to stop these attacks before they start.

Signs You're Emailing a Fraudster

"Bad actors are targeting Gmail, Microsoft, and Yahoo accounts that lack multi-factor authentication (MFA). If you have not set up two-factor authentication in your email, we highly recommend you do that now."

MICHAEL GRACE

VP OF CUSTOMER RISK MANAGEMENT AT HIGHWAY

Red flags to watch out for:

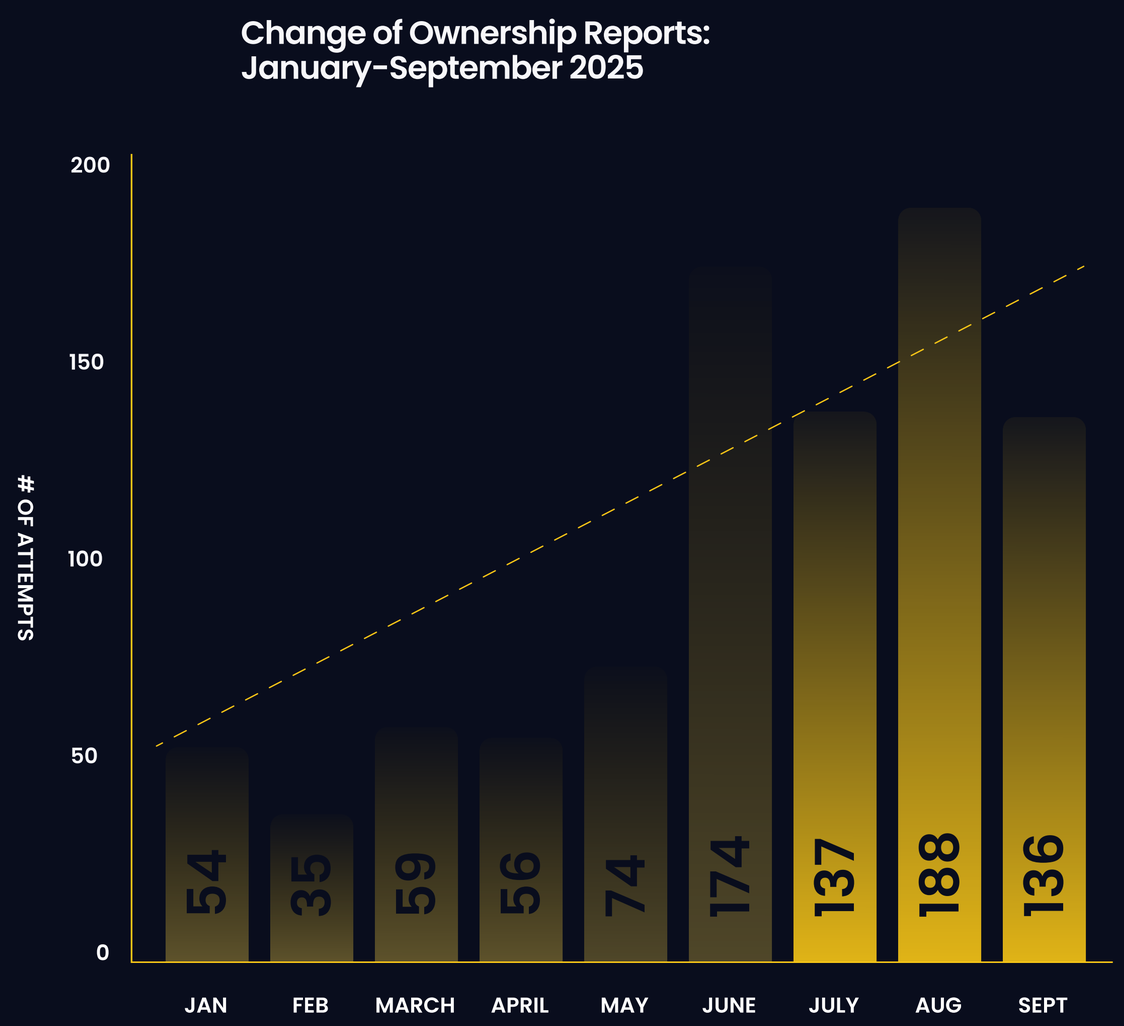
- Emails from familiar contacts that arrive from a different or slightly altered domain.
- Last-minute changes that demand urgency or new payment/route instructions.
- A carrier that usually answers calls but only responds by email that day.
- Rate confirmations sent as PDFs in email attachments rather than requiring the receiver to go through an identity authenticated system.

2

Sold MCs & Ownership Changes

Ownership-change manipulation, often referred to as “Sold MC” activity, remains one of the most persistent forms of fraud in freight. After a spike in the first half of the year, Q3 data shows a measurable decline in new alerts reported by Highway, suggesting growing awareness across the industry and stronger front-line defenses by brokers and compliance teams.

These schemes typically involve fraudsters acquiring or taking over legitimate MC numbers and using the carrier’s established reputation to access loads, secure payments, and conceal theft. The transition can appear legitimate on paper, making it difficult to detect without continuous monitoring of behavioral, registration, and insurance changes.



Q3 2025 Trend

Patterns Behind Ownership Changes

Red flags to watch out for:

- Insurance updates with *sudden coverage* shifts that don't align with the carrier's past operations.
- Ownership transfers tied to *clusters of suspicious activity* rather than isolated changes.
- Login behavior that reveals *new users accessing accounts from unfamiliar geographies.*
- Dispatch activity that looks *unnatural*—carriers picking up in regions far outside their normal lanes.

Staying Ahead of Sold-MC Schemes

Highway's Carrier Identity® Engine continuously tracks and flags ownership irregularities by analyzing behavioral shifts, registration changes, and insurance updates in real time. When anomalies are detected, Highway automatically escalates these profiles for re-verification through its Identity Proofing process.

This approach ensures that only verified carriers remain active in broker networks, helping brokers identify potential bad actors before they can exploit newly acquired or compromised MC numbers. While volumes declined by 21% from late Q2 to early Q3, ownership-change abuse remains one of the most persistent fraud tactics in the market, reinforcing the need for continuous monitoring, alert response, and strict adherence to verification protocols.

Best Practices for Brokers and Compliance Teams:

- **Watch for unusual patterns.**
  Sudden insurance changes, new equipment, new phone numbers, or login activity from different regions can indicate a MC takeover.
- **Investigate all change-of-ownership alerts.**
  Verify supporting documentation directly with the carrier and confirm legitimacy of new contacts.
- **Require re-verification before booking.**
  Treat every ownership change as a temporary red flag until proven otherwise.
- **Maintain ongoing education.**
  Teams should understand what a sold-MC pattern looks like and escalate questionable activity immediately.

3

Direct Theft by Rogue Carriers

While total theft volumes declined slightly quarter over quarter, direct thefts grew as a share of overall incidents — a sign that rogue carriers are evolving their tactics.

Highway data shows that shell entities and carriers operating under multiple MC numbers were most often tied to theft cases, often exploiting trust built through legitimate prior moves.

Michael Grace, VP of Customer Risk at Highway, notes that these “rogue carriers” are increasingly pilfering partial loads, falsifying proof-of-delivery documents, or disappearing entirely with freight — highlighting the need for brokers to maintain continuous monitoring even after a load is booked.

The Rise of Rogue Carriers

Rogue carriers are increasingly infiltrating legitimate freight networks, pilfering loads, falsifying proof-of-delivery documents, or vanishing entirely with freight.

This rise coincides with tightening federal oversight on non-domicile CDLs, which Grace believes is creating short-term openings for opportunistic actors posing as compliant carriers. These individuals often exploit familiarity with shipper and receiver routines, leveraging prior legitimate hauls to mask theft attempts until long after delivery.

> "These carriers learn shipper and receiver routines — who asks for which pickup numbers, which PODs can be altered and not found out for six months — and then they act."

MICHAEL GRACE
VP OF CUSTOMER RISK MANAGEMENT AT HIGHWAY

Common Patterns

- Partial delivery followed by altered PODs.
- Loads stolen outright after pickup, especially high-value or perishable goods.
- Pilferage during multi-stop routes, particularly for beverage, alcohol, and consumer goods.

Commodities Most Targeted in Q3

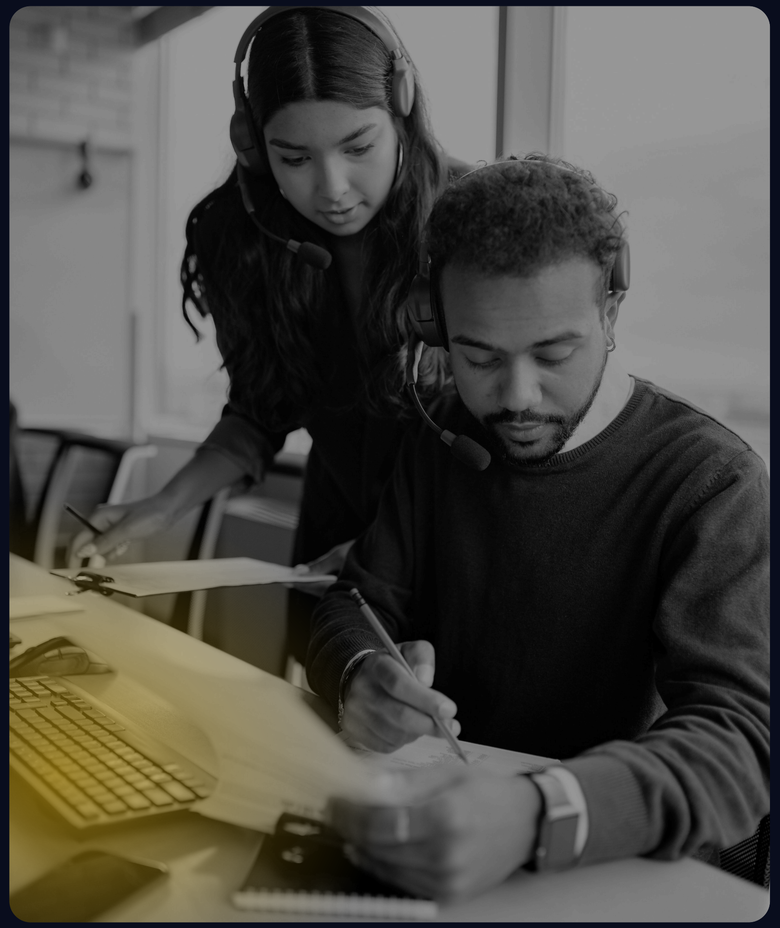
- Meat & Seafood (notably rising in August and September)
- Electronics and consumer technology
- Alcoholic beverages and bulk packaged goods

Back To The Basics On Fraud Prevention

Even as fraud tactics grow more sophisticated, Highway's Q3 analysis shows that most thefts remain entirely preventable through disciplined adherence to proven fundamentals. The most effective defense still lies in the basics—vigilance, verification, and communication across every stakeholder in the freight transaction.

Fraud Prevention Checklist

For Brokers



1

Verify every booking through an outbound call. Treat email as a signal, not proof. Always confirm critical requests with an outbound phone call.

2

Spot-check every contact. Validate email domains and phone numbers through an identity platform like Highway before booking.

3

Secure rate confirmations with two-factor authentication and digital acceptance rather than email attachments to protect sensitive load information that bad actors seek.

4

Monitor for unusual account behavior (overbooked, unexpected changes to insurance or ownership) and force re-verification when anomalies appear.

5

Confirm delivery directly with your shipper customers

6

Report suspicious activity immediately to your compliance team and Highway. Rapid response can aid recovery.

Fraud Prevention Checklist

For Carriers

1

Verify every broker’s legitimacy before accepting a load. Confirm company details and contact info through trusted sources.

2

Enable two-factor authentication (2FA) on your email to protect against inbox compromises.

3

Cross-check all load details against tender documents and rate confirmations—never rely on email instructions alone.

4

Monitor your business accounts for unusual or unauthorized activity.

5

Keep your insurance and registration current to avoid being flagged during verification.

6

Inspect equipment and ensure compliance with all tender requirements before pick up.

Fraud Prevention Checklist

For Shippers

1

Inspect trucks at pickup. Watch for red flags such as zip-tied plates, reversed hinge bolts, mismatched VINs, or signs of neglected maintenance.

2

Verify driver identity and carrier information. Cross-check the driver's name, CDL, and company details against the BOL and tender documentation.

3

Confirm seals, locks, and vehicle condition at both pickup and delivery. Ensure seals match paperwork and note any discrepancies immediately.

4

Document everything. Capture photos of the truck, trailer, and seal numbers at pickup and delivery for recordkeeping.

5

Report any mismatches or suspicious behavior to both the broker and Highway immediately.

6

Avoid unverified substitutions. Never release freight to a carrier, driver, or vehicle that was not authorized by the broker of record.

Fraud Prevention Checklist

For Insurance Agencies

1

Verify carrier legitimacy and coverage before issuing or renewing any policy. Confirm operating authority, MC/DOT status, and policy validity through trusted data sources.

2

Monitor for ownership or authority changes. Frequent ownership transfers, reinstatements, or name changes are key red flags for identity fraud and policy abuse.

3

Track and review claims activity. Look for unusual frequency, timing, or patterns (e.g., multiple claims right after reinstatement or ownership change).

4

Require real-time compliance updates via trusted platforms like Highway to maintain verified insurance and compliance data to reduce risk.

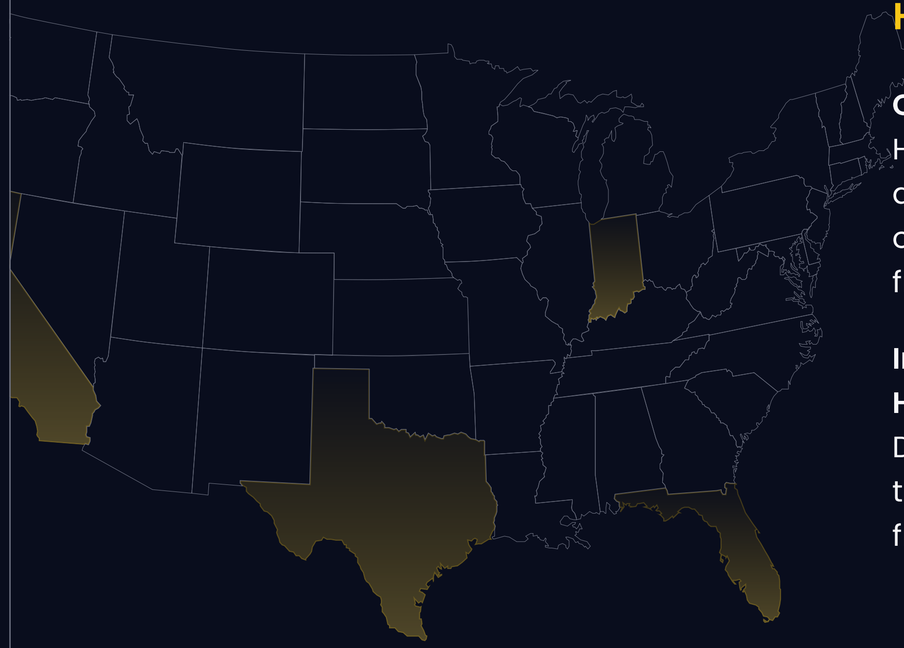
5

Educate clients on fraud trends. Share prevention best practices with carriers and brokers to strengthen network-wide protection.

Q4 Seasonal Threat Watch

Heightened Theft Risks During Holiday Season

The holiday surge in freight volume brings increased risk for fraud and cargo theft. Awareness and vigilance are key as opportunistic actors target high-value, fast-moving goods across key markets.



High-Risk Regions

California, Texas, Florida: High-volume ports, warehouses, and retail centers create more opportunities for theft and fraudulent carrier activity.

Indiana & Midwest Distribution Hubs (Indianapolis, Greenwood): Dense consolidation points make these areas susceptible to identity fraud and compromised carriers.

High-Risk Commodities

Meat, Seafood & Frozen Goods
Demand spikes around Thanksgiving and year-end holidays make perishable, high-value food shipments prime targets.

Consumer Electronics & Premium Retail Items
Easy to resell and often shipped in bulk, these loads remain a top target for diversion and fictitious pickups.

Alcohol & Beverages (Bulk)
Seasonal distribution surges drive higher movement of alcohol and specialty beverages, creating additional exposure.

Identity-First Protection In Action

How Highway Protects the Lifecycle of the Load

Highway secures every stage of the load with an identity-first approach that begins before a transaction starts. Carriers must prove who they are, their authority to operate, and their equipment, giving brokers confidence that they are working with verified partners. Protection continues through the entire lifecycle of the load with continuous monitoring, adaptive compliance checks, and real-time fraud detection.

Secure Rate Con Delivery safeguards tenders from inbox spoofing and phishing attempts, while ELD-verified tracking confirms that the right truck is moving the right load to the correct destination. From onboarding through delivery, Highway provides complete visibility and protection so brokers can move freight with transparency, speed, and trust.

See How Highway Protects Every Load From Start To Finish

Schedule a Demo ↗

highway.com