HIGHWAY

Q2 2026

FREIGHT FRAUD INDEX REPORT

The New Rules of Trust

April – June 2026

highway.com

FREIGHT FRAUD INDEX

From the Risk team

Fraud does not disappear. It adapts. So must we.

The Freight Fraud Index is built from Highway Risk team investigations, customer-reported theft events, platform data, and the industry developments shaping each quarter. Our goal isn't to catalogue every fraud event — it's to explain what changed, why it matters, and how brokers should adapt.

The numbers in this report support the findings. They don't define them. Fraud is dynamic, and understanding why it's changing matters as much as how often it occurs.

The common thread this quarter is clear: **trust is changing**. As regulators strengthen identity requirements and brokers adopt stronger verification, fraudsters are shifting from creating fake identities to exploiting the trust that already exists — relationships, communication channels, and operational processes.

Technology keeps getting better at surfacing risk. But technology alone can't replace sound operational judgment. The organizations that combine both will stay ahead.

FREIGHT FRAUD INDEX

Executive Summary

In Q2 2026, trust itself became the attack surface. Communication-based attacks — compromised inboxes, spoofed emails, account takeovers, impersonation calls — accounted for 50% of all classified fraud vectors, up from 42.7% in Q1. Highway blocked 784,201 fraudulent inbound emails and 109,995 fraudulent or spoofed phone calls, both up roughly 50% quarter over quarter. And fraudsters started impersonating Highway itself: phishing and impersonation activity jumped 282%.

Behind the numbers, the rules of trust are being rewritten. The FMCSA's transition to Motus is raising the bar for who can establish a carrier authority. The Supreme Court's decision in *Montgomery v. Caribe Transport II, LLC* is raising the bar for broker diligence.

Continued ELD enforcement is raising the bar for operational accountability. That's progress — but stronger controls don't eliminate fraud. They relocate it. As creating fraudulent identities gets harder, fraud is moving toward inheriting and exploiting trust that already exists: sold MCs, ownership changes, and the communication channels brokers rely on every day.

The message for brokers is unambiguous: verification is not a one-time event. Identity, ownership, communication, and operational behavior all contribute to whether a carrier relationship can be trusted at the moment freight moves. The brokers reducing their exposure are the ones validating trust through the entire carrier lifecycle — not just at onboarding.

Why this matters

Authority age, years in business, and safety history have long served as proxies for trust. They're still valuable — but the trust attached to an authority can change as ownership, operations, and communication practices change. The industry is moving from one-time qualification to continuous validation. Long-standing carriers aren't inherently risky. Static trust is.

Q2 2026 IN REVIEW

Trust got a higher bar. Fraud found a side door.

Three developments reshaped how trust is established this quarter.

1. The FMCSA's transition to **Motus** introduces stronger identity verification at carrier registration — a higher standard for confirming who is behind a new authority.
2. The Supreme Court's ***Montgomery v. Caribe Transport II, LLC*** decision — a unanimous ruling on May 14 that negligent-hiring claims against brokers are not preempted by federal law — increased the scrutiny placed on how brokers evaluate and qualify carriers before tendering freight.
3. The FMCSA continued **decertifying ELD providers** that fail federal standards — 15 providers revoked in Q2 alone.

Each raises the standard for legitimate operators. Each also changes where fraud concentrates. History is consistent on this point: stronger controls don't make fraud disappear — they change where fraudsters focus their effort. When creating trust gets harder, stealing it gets more attractive.

That's exactly what Q2 showed. Fraudulent identity creation declined as registration controls tightened. Meanwhile, every measure of trust exploitation climbed: compromised inboxes, spoofed communications, account takeovers, and ownership-change fraud.

INSIDE THE Q2 FRAUD LANDSCAPE

What's trending down, what's trending up

Fraud pressure on communication channels accelerated again in Q2 — across email, phone, and the trust signals in between.

Not every line went up. Ownership-discrepancy alerts fell 40.9% — even as ownership's share of theft reports rose — and fraudulent identity creation kept declining as registration controls tightened. Read carefully, that's not fraud receding. It's fraud relocating: away from fabricated identities, toward the trust you've already extended.

48.5%

QoQ increase in fraudulent inbound emails blocked

784,201; +58.3% vs Q2 2025

53.2%

QoQ increase in fraudulent and spoofed phone calls blocked

109,995; +159% vs Q2 2025

282%

QoQ increase in Highway-impersonation and phone-phishing activity

1,740 list additions

Q2 2026 Freight Fraud Trends

368

Carrier Users

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

784,201

Fraudulent Inbound Emails Blocked

13,746

Unauthorized FMCSA contact changes

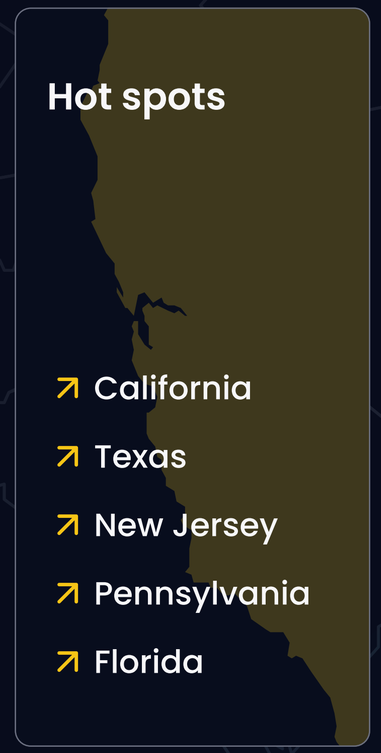
109,995

Fraudulent and Spoofed Phone Calls Blocked

245

Change in Ownership Reports

Hot spots



- California
- Texas
- New Jersey
- Pennsylvania
- Florida

Top Countries

India | Pakistan | Serbia

Top targeted commodities

General Merchandise | Bulk | Non-Perishable Food & Beverage

Based on Highway App, Inc. data from April – June 2026. "Fraudulent inbound emails blocked" = inbound emails classified as spoofing attempts or flagged for fraud (email or domain). "Fraudulent and spoofed phone calls blocked" = inbound calls flagged for fraud, from blocked users/companies, unknown high-risk numbers, or known numbers not belonging to the carrier.

TOP Q2 FRAUD VECTORS

Where trust was exploited

Q2 2026 • TOP FRAUD VECTORS

Compromised communications

Half of all classified fraud vectors in Q2 were communication-based, increasing from 42.7% in Q1 to 50% in Q2. Across Highway investigations, one pattern emerged consistently: fraud rarely succeeded because a carrier couldn't be identified. It succeeded because a trusted communication channel was compromised, misused, or relied upon without independent validation.

Once a fraudster controls an inbox or spoofs a phone number, they don't need to defeat your security controls. They need you to trust the communication.

The Numbers Behind the Trend

109
theft investigations linked to compromised inboxes

91
stolen loads during Q2

Highway also observed account takeover emerge as a new fraud vector, reinforcing a broader trend: fraud is increasingly targeting trusted communication channels rather than creating entirely new identities.

The takeaway is clear.

Verifying who a carrier is remains essential. Increasingly, the more important question is whether the person communicating on that carrier's behalf is authorized to do so.

50%

of classified fraud vectors originated through compromised communications

“Almost every successful theft starts with a bad actor exploiting your trust. They're counting on a compromised contact method to appear legitimate and hoping your process won't detect the deception before the freight is gone.”

DEMI RAMON
VP of Risk

HIGHWAY

Q2 2026 TREND

Don’t trust the channel. Verify the person.

Unexpected operational changes aren’t automatically suspicious. Businesses add dispatchers. Phone numbers change. FMCSA records are updated. New email addresses are created every day.

What matters isn’t whether change occurred. It’s whether the change was independently verified. Every unexpected change should trigger validation through communication channels you’ve already established — not the ones introduced during an active transaction.

Best Practices

- **Verify through established contacts.** When communication details change during a transaction, confirm the change through the carrier’s historically established contacts rather than the channel requesting the update.
- **Train for impersonation.** Highway will never call and request a verification code. As impersonation activity increases, every employee — including after-hours operations staff — should understand how these campaigns work.
- **Secure your rate confirmations.** Authenticated delivery workflows such as Secure Rate Con Delivery reduce reliance on unsecured email attachments. Adoption accelerated across the network in Q2.
- **Treat familiarity as a risk — not proof.** A compromised inbox looks exactly like the legitimate one. Reply history should never replace independent verification.

Q2 2026 • TOP FRAUD VECTORS

Ownership changes and inherited trust

Change-in-ownership accounted for 25.6% of reported thefts during Q2, up from 23.0% in Q1, even as ownership discrepancy alerts declined 40.9%. That divergence tells an important story: the ownership fraud that remains is becoming more difficult to detect because it often involves authorities with years of operating history, established broker relationships, and otherwise legitimate operating signals. **The authority hasn't changed. The people behind it have.**

Ownership transitions happen every day for legitimate business reasons. The challenge is recognizing when the trust associated with an authority no longer reflects its current operational reality.

To strengthen visibility into these changes, Highway introduced Ownership Attestation during Q2. When material ownership changes are detected, historically associated owners are asked to affirm whether ownership has changed — providing an additional layer of accountability before traditional data sources reflect those updates.

The takeaway

A sold MC rarely appears suspicious. It often looks like a carrier you've trusted for years. That's precisely what makes continuous validation essential.

25.6%

of reported thefts involved ownership change

Highway's position

These observations warrant continued monitoring. They should not be interpreted as a standalone determination of fraud, and no single shared attribute should define carrier risk.

Instead, these signals provide additional context that should be evaluated alongside identity, ownership, communication, and operational behavior. This remains an intelligence watch — not a solved detection category.

INTELLIGENCE WATCH

Chameleon carriers

Highway continues to monitor an emerging set of operational patterns commonly referred to as chameleon carriers — carriers that appear distinct on paper while sharing equipment, identity information, or other recurring characteristics across multiple authorities.

This remains an area where the industry should avoid overstatement. Shared operational characteristics often have legitimate explanations, including affiliated entities, equipment leasing, administrative errors, or normal business transitions. No single indicator should be interpreted as evidence of fraud. Even so, recurring patterns deserve attention.

During the first half of 2026, Highway observed:

41,016 VINs appearing on insurance certificates for more than one carrier. Of those, 2,907 appeared across three or more carriers, 119 across five or more, and one VIN appeared across 48 different carriers.

Recycled VINs associated with fraud alerts appearing on insurance certificates for more than one carrier. Of those, 2,907 appeared across three or more carriers, 119 across five or more, and one VIN appeared across 48 different carriers.

9,836 identity documents were associated with more than one Highway user account, with 1,538 spanning multiple carrier authorities. The most significant example involved a single document appearing across 356 accounts and 270 carriers.

Q2 2026 TREND

The diligence standard is rising

The Supreme Court's decision in *Montgomery v. Caribe Transport II,* LLC didn't create new regulations. It changed expectations. Combined with the FMCSA's Motus transition and continued ELD enforcement, one message is becoming increasingly clear: "we verified them during onboarding" is no longer enough.

The standard for reasonable diligence continues to evolve, requiring brokers to validate trust throughout the carrier relationship — not just before the first load moves. Across Highway investigations, organizations that consistently reduced fraud exposure shared several common practices. Not because they adopted a single technology — because they operated with discipline.

Broker responsibility

Technology can surface risk. Technology cannot create operational discipline. The strongest fraud prevention programs pair technology with documented policies, consistent review procedures, and disciplined exception handling. The tools continue improving. Judgment remains the broker's responsibility.

What reasonable diligence looks like

- **Qualification is documented — not assumed.** Carrier selection criteria are clearly defined, consistently applied, and documented on every load — including the ones booked late on a Friday afternoon.
- **Exceptions follow a documented process.** When a carrier falls outside established criteria, someone with appropriate authority reviews the exception and documents the decision. Exception handling is often where fraud succeeds.
- **Operational changes trigger re-validation.** New contacts, insurance changes, ownership updates, or equipment changes should reset the validation process regardless of how long the carrier relationship has existed.
- **Internal identity matters, too.** Identity discipline doesn't stop with carriers. One employee should have one login. Shared accounts and borrowed credentials reduce accountability and make post-incident investigations significantly more difficult.

Q3–Q4 • SEASONAL THREAT WATCH

Peak season is fraud season

The second half of the year consistently creates conditions that favor fraud. Labor Day marks the beginning of that cycle, bringing lighter staffing, increased freight volume, and slower response times. As peak shipping season accelerates, brokers face greater pressure to move freight quickly, onboard unfamiliar carriers, and make operational decisions under tighter timelines.

Fraudsters understand those pressures. They don’t create urgency. They exploit it. Throughout peak season, social engineering campaigns become more effective because they rely on operational pressure: after-hours calls claiming to represent the assigned carrier, last-minute reroute requests, updated contact information, and situations designed to encourage teams to bypass established verification procedures.

Volume isn’t the risk. Compromising operational discipline is.

Q3–Q4 • SEASONAL THREAT WATCH

Preparing for peak season

Don’t let volume lower your standards.

Apply the same carrier qualification process to every load, especially when capacity is tight.

Treat reroutes as high-risk events.

Verify every delivery change through trusted broker contacts and require updated written authorization before freight moves.

Prepare your operations teams before Labor Day.

Review current fraud tactics, escalation procedures, and verification workflows with weekend and after-hours staff before peak season begins.

Revalidate unexpected changes.

Last-minute updates to contacts, FMCSA records, ownership information, or dispatch instructions should always trigger additional verification.

Q3 2026 • FRAUD FORECAST

Where trust will be tested next

As registration controls strengthen and expectations for broker diligence continue to rise, fraud will increasingly concentrate where trust remains most difficult to validate. **During the second half of 2026, Highway expects continued emphasis in three areas:**

1

Communication integrity. Compromised inboxes, spoofed domains, account takeovers, and impersonation campaigns will continue targeting the communication channels brokers rely on to verify carrier identity.

2

Inherited trust. Ownership changes, sold MCs, and long-standing carrier relationships will remain attractive because they leverage trust that has already been established rather than creating entirely new identities.

3

Operational manipulation. Fraudsters will continue focusing on reroutes, unauthorized communication channels, dispatch changes, and payment workflow manipulation rather than traditional identity creation schemes.

Organizations best prepared for this shift will validate trust continuously — across identity, ownership, communication, and operational behavior — rather than treating verification as a one-time onboarding event.

> **“Identity establishes trust. Continuous verification preserves it. In today’s freight market, both are essential on every load.”**

DEMI RAMON
VP of Risk
HIGHWAY

Q2 2026 FREIGHT FRAUD INDEX

Key takeaways

What Q2 revealed

The standards for establishing trust continue to evolve. Identity creation is becoming more difficult. Identity exploitation is becoming more common.

Communication-based fraud now represents half of all classified fraud vectors. Ownership-change fraud continues to grow even as traditional alerts decline. Together, these trends reinforce a broader shift: fraud is increasingly targeting trusted relationships, communication channels, and operational processes rather than creating entirely new identities.

Fraud isn’t disappearing. It’s relocating.

Highway’s perspective

Fraud prevention is no longer the responsibility of any single broker, carrier, or technology platform. It depends on a network of shared intelligence, continuous verification, and disciplined operational decision-making.

Every suspicious identity reported through Highway strengthens that network. Every verified signal helps another broker make a more informed decision before freight moves.

Technology alone doesn’t create trust. People do. Technology helps them validate it.

FREIGHT FRAUD INDEX

The new rules of trust

Every quarter changes the tactics. Q2 changed something larger. It changed the standard.

Identity alone is no longer enough. Communication alone is no longer enough. Operational history alone is no longer enough. Trust now depends on continuously validating who a carrier is, who is acting on that carrier's behalf, and whether operational behavior continues to align with the relationship you've established.

The organizations that will reduce fraud over the next decade won't simply respond faster. They'll build operating models that continuously validate trust. That's where the industry is headed. Highway intends to help define that standard.

Fraud will continue to evolve. So will we.

If you experience fraud or suspicious activity, report it to **reportfraud@highway.com.**

To learn how Highway helps brokers continuously validate trust throughout the carrier lifecycle, schedule a demo at **highway.com.**


HIGHWAY
highway.com