HIGHWAY

Freight Fraud Index Report Q2 2025

An Industry Overview of Cargo Theft, Broker Scams, and Risk Mitigation Trends

Freight Fraud Index

Inside Today’s Freight Fraud Tactics

Freight fraud is no longer just opportunistic. It’s organized, adaptive, and alarmingly sophisticated. Today’s bad actors aren’t always breaking in; they’re blending in. They pose as real carriers, operate legitimately to learn your network, and strike when your guard is down. From inbox takeovers to sold MC scams, fraudsters are exploiting digital and physical blind spots across the supply chain.

In this edition of the Freight Fraud Index, we break down the most active fraud vectors Highway is tracking, how they’re evolving, and what brokers and carriers need to do now to stay ahead.

Q2 2025 Freight Fraud Trends

700

carrier users from 40 countries

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

Top Countries

India | Pakistan | Serbia

495,267

Fraudulent Inbound Emails Blocked

289

Unauthorized FMCSA Contact Changes

42,421

Fraudulent Phone Calls Blocked

2,281

Fraud-Related Identity Alerts Reported

Based of Highway App, Inc. data from April - June 2025

Mid-Year Update

Q2 Hit Hard.

In the first half of 2025, identity-based freight fraud has continued to surge, with bad actors layering multiple tactics into single attacks. Highway saw a **23% increase in broker-reported identity fraud** in Q2 compared to Q1, and a **41% spike in blocked attempts across email and phone**.

By June 2025, Highway has already blocked 847,401 fraudulent attempts for their broker customers—**92% of last year's total in just six months.**

Spoofed emails, stolen MCs, and compromised inboxes are no longer isolated threats, they're increasingly being used together to bypass broker defenses. Here's a recap of the top fraud vectors in 2025.

847,401

Total Fraudulent Attempts Blocked in 2025

92% of 2024's Total

3,471

Broker-Reported Identity Alerts in 2025

29% of 2024's Total

TOP Q2 FRAUD VECTORS

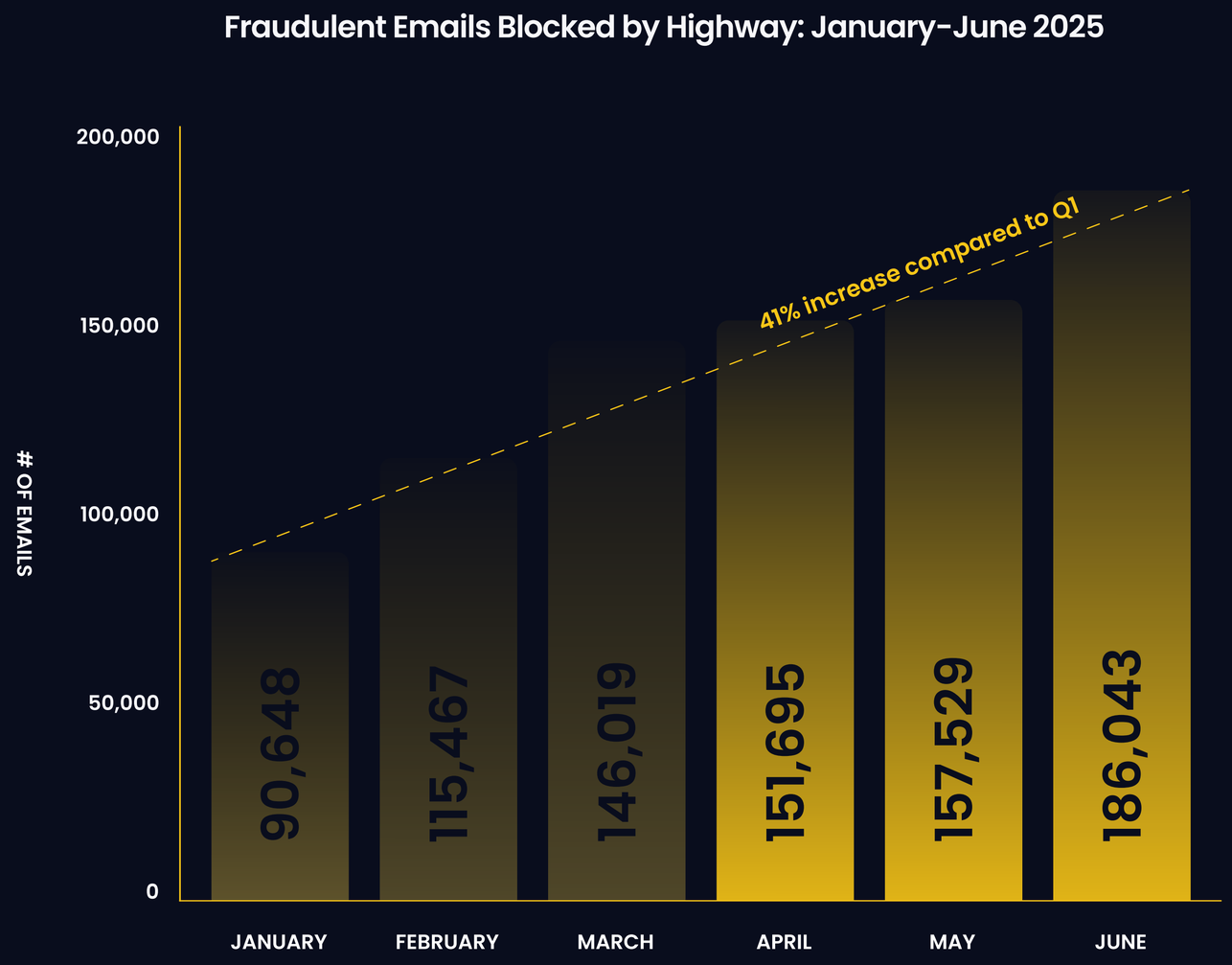
The New Patterns Driving Fraud

1 Compromised Inboxes

Your team can do everything right: vet the carrier, confirm insurance, double-check documents and still lose a load. One of the ways fraudsters slip through undetected is by hijacking a legitimate carrier's inbox.

How the Deception Works:

- A fraudster tricks a real carrier into entering their credentials on a fake login page through a phishing scheme.
- Now inside the inbox, the attacker monitors communication silently—watching for rate confirmations, sensitive documents, or any opportunity to intercept a transaction.
- Take a rate con, for example. When a broker sends a rate con, the attacker deletes the email and uses the information to impersonate the carrier.
- With the paperwork in hand, they show up at pickup and steal the freight before anyone realizes what happened.



Q2 2025 Trend

Compromised Inboxes Are Fueling Theft

We've seen a sharp increase in fraudsters breaking into email accounts to impersonate real carriers and dispatchers. Most attacks target Gmail, Microsoft, or Yahoo accounts without Multi-Factor Authentication (MFA). **In Q2 alone, Highway blocked 41% more** fraudulent email attempts than in Q1. These attackers used realistic dispatch names, spoofed domains, and fully compromised inboxes to reroute payments, intercept rate confirmations, and steal freight.

Best Practice

Secure Your Rate Confirmations

To shut down this attack vector, Highway launched Secure Rate Con Delivery in Q2. This feature requires the carrier's authorized user to re-authenticate using multi-factor authentication before accessing a rate confirmation, just like banks do for sensitive financial statements.

Even if a fraudster has access to the inbox, they won't have access to the verified user's phone and that means your load data stays secure and your freight stays protected.

"While carrier email security is beyond our control, we can control access to their Highway account. This makes Highway's Secure Rate Con Delivery the most secure option for protecting against compromised emails."

MICHAEL GRACE
VP OF CUSTOMER RISK MANAGEMENT AT HIGHWAY

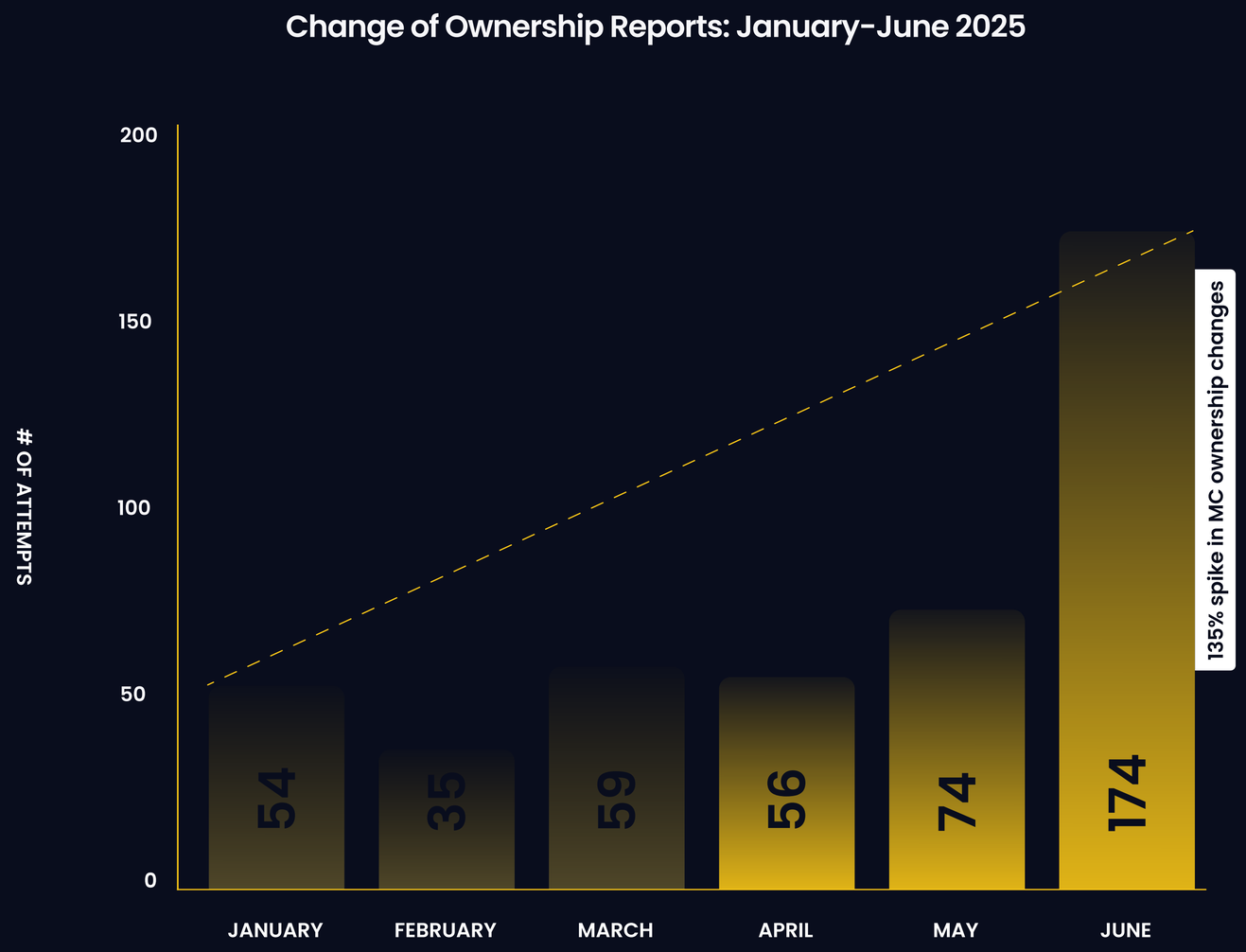
2

Sold MCs & Ownership Changes

Sold MCs present one of the most deceptive forms of freight fraud. On the surface, everything appears legitimate: the MC has clean safety history, long-standing broker relationships, active logins, and legitimate insurance.

But these bad actors are not just buying an MC. They're buying the entire identity: the phone number, email address, business bank account, and even a copy of the previous owner's CDL. With those credentials in hand, fraudsters can impersonate the original carrier and operate undetected—often for weeks—before the first red flag is ever raised.

In one case, eight cargo theft claims had to be filed before the insurance provider contacted the original MC owner—who had no idea his identity was still being used.



Q2 2025 Trend

Sold MCs is a Silent Threat

In June 2025, there was a **135% spike in suspicious MC ownership changes** connected to cargo theft reports, signaling that this vector is accelerating and not slowing down.

Because the MC looks healthy on paper, brokers and shippers often miss the warning signs of a change of ownership.

Here are some common red flags to be aware of:

- A dormant carrier suddenly reactivates after 2–6 months
- Insurance updates to a new producer or VIN doesn't match
- Contact information changes but doesn't align with prior data
- Logins from unfamiliar locations or IP addresses
- Sudden urgency around payment or dispatch changes

Best Practice

Don’t Just Trust the MC—Verify Who’s Behind It

Surface-level checks like insurance, safety score, or authority status aren’t enough to catch a Sold MC. The only way to detect ownership changes or unauthorized control is to verify the person behind the login—not just the company name on paper.

Highway helps brokers go deeper by monitoring identity signals, communication behavior, and load-level compliance.

Because when MCs are bought, sold, or hijacked, the risk isn’t just hidden—it’s active.

> “If you don't know who you're working with, you're giving fraud a head start. Identity checks should be standard, not optional.”

MICHAEL GRACE
VP OF CUSTOMER RISK MANAGEMENT AT HIGHWAY

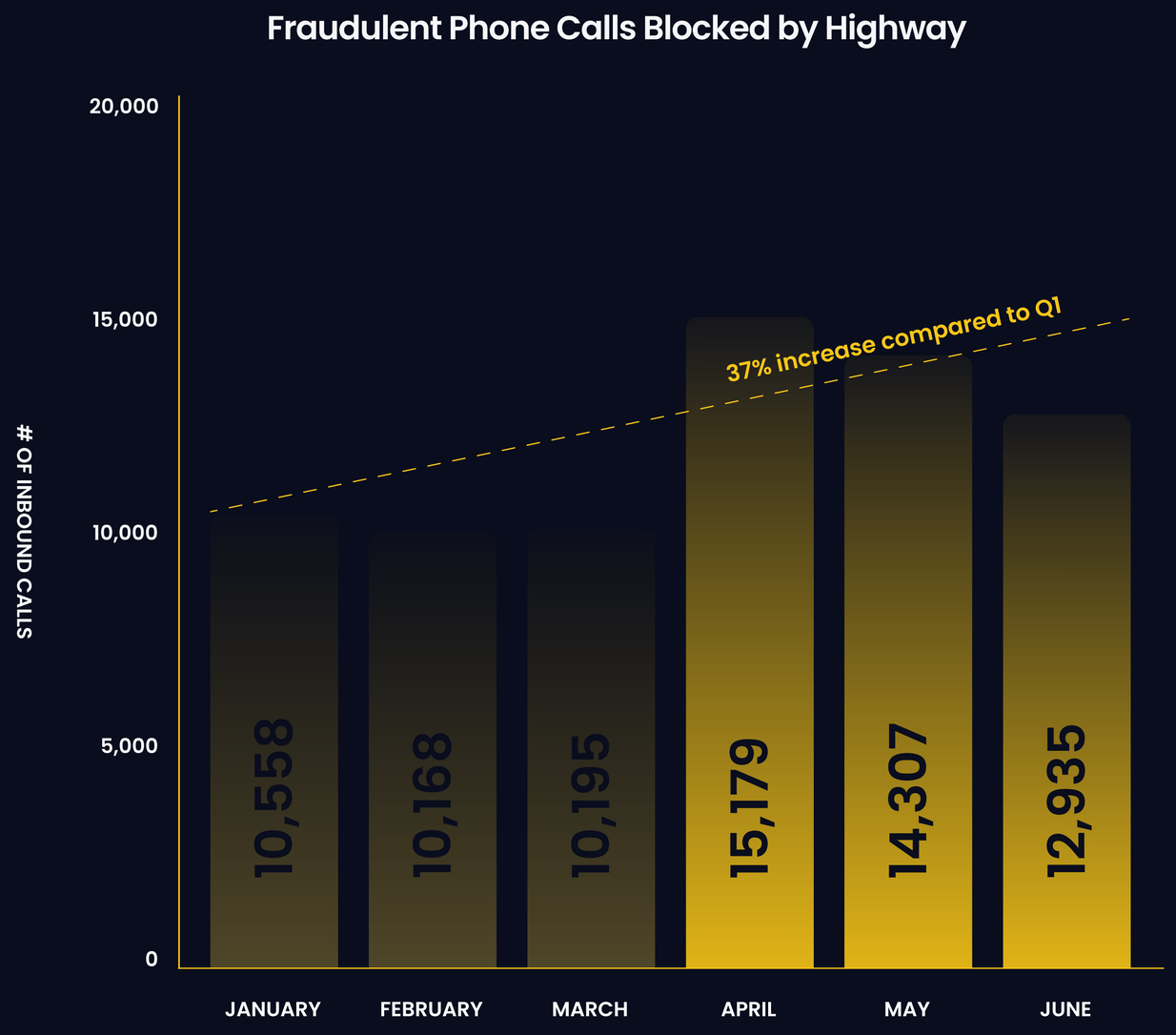
3

Phone-Based Identity Fraud

This isn’t telemarketing noise—it’s a targeted fraud vector designed to breach your network.

Fraudsters manipulate a legitimate carrier’s phone number and name on caller ID to appear credible. Once they get a broker on the phone, they often request rate confirmations or provide a new email address (one not authorized by the real carrier) to divert communication and secure a load under false pretenses.

This fraud vector is especially effective when brokers post loads to public boards. The fraudster doesn’t need to hack into a system, they just need a phone number, a convincing voice, and a target who assumes what they see on caller ID is real.



Q2 2025 Trend

Fraudulent Inbound Calls Continue to Escalate

Between April and June 2025, **Highway blocked over 42,000 fraudulent inbound calls, a 37% jump from Q1**. The trend is clear: freight fraud rings are increasingly manipulating caller identities to gain access to loads and sensitive information.

To Mitigate Phone-Based Fraud:

- Never trust caller ID at face value. Fraudsters often spoof real carrier numbers to appear legitimate.
- Avoid using contact information provided over the phone unless verified. Always cross-reference with known, trusted sources like Highway.
- Require identity verification before sharing sensitive information. Confirm that the caller has the authority to represent the carrier they claim.
- Watch for urgent requests. Fraudsters often pressure teams to act quickly—slow down and verify.

Best Practice

Block Fraudulent Calls Before They Reach Your Team

Highway for VoIP proactively detects and blocks fraudulent calls before they reach your carrier sales team. Built directly into your IVR system with zero disruption, it uses Highway's Identity Engine to verify that every inbound call aligns with a known, verified carrier. Suspicious numbers are automatically routed out of your network, reducing the risk of engagement with bad actors.

By combining best practices with purpose-built technology, you create a layered defense that protects your team and ensures you're only speaking with verified, trusted carriers.

"Phone is one of the most overlooked entry points for fraud. With Highway for VoIP, brokers don't just answer fewer bad calls—they eliminate the threat before it ever rings."

MICHAEL GRACE
VP OF CUSTOMER RISK MANAGEMENT AT HIGHWAY

LONG WEEKENDS TARGETED

Fraud During Memorial Day Weekend

50% of reported thefts during May 2025 occurred the week of Memorial Day (May 26-30)

Long weekends create ideal conditions for freight fraud due to lighter staffing and increased freight volume. They exploit slower response times, leaner weekend coverage, and a surge in high-value freight to steal loads that contain particularly perishables, electronics, and seasonal inventory.

How to strengthen your defenses during the holidays:

Trust your instincts and verify

If it feels off, verify before sharing load info or dispatching.

Watch for last minute MC changes

Fraudsters often manipulate FMCSA records right before a scam. Look for sudden contact or status shifts.

Know your high-risk window

Risk peaks Friday afternoon to Monday evening. Watch for spoofed logins and sketchy communications.

Prep your team before the weekend

Brief your operations team on the latest fraud tactics, red flags and how to escalate suspicious activity.

Q3 2025 Fraud Forecast

Bad Actors Study Patterns Before They Strike.

Fraudsters are becoming more targeted and calculated. They're not just attacking—they're observing. They look for gaps across communication channels and wait for the right moment to strike. They monitor patterns, track where loads are posted, and exploit timing to slip in undetected.

Protecting your team requires real-time identity verification at every point of interaction: phone, email, and onboarding. Use verified contact methods. Secure your rate confirmations behind multi-factor authentication. Question any sudden change in ownership, insurance, or communication behavior.

“Fraud today isn’t loud—it’s calculated. Bad actors study your patterns, wait for gaps, and strike when you least expect it. That’s why identity verification at every touch point isn’t optional—it’s essential.”

Michael Grace, VP of Customer Risk Management at Highway

Fraud Won’t Wait. Neither Should You.

Freight fraud isn’t going away, but with the right identity-based protections, it doesn’t have to reach your network. With Highway’s Carrier Identity® and fraud prevention solutions, you can keep your network secure from the first carrier interaction to final delivery.

The teams staying ahead are securing every touchpoint, questioning anomalies, and relying on proof—not assumptions. Stay vigilant. Stay proactive. And most of all, trust only what can be verified.

highway.com