HIGHWAY

Freight Fraud Index Report Q1 2025

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

Freight Fraud Index

Inside The Evolving Fraud Playbook

Strategic fraud and cargo theft in the freight industry isn't slowing down — it's evolving.

As fraud rings adapt, they're targeting the soft spots: overlooked verifications, siloed systems, and gaps in communication security. The Q1 2025 Freight Fraud Index pinpoints the latest fraud threats and shows brokers how they can respond.

2024 in Review

Fraud Hits a New Gear

2024 marked a turning point for fraud in freight — with a 27% increase in fraudulent activity year-over-year[1] targeting freight brokers, carriers, and shippers.

27% Increase in Fraudulent Activity (2024)

914,719

Blocked Fraud Attempts

Highway blocked 914,719 fraud attempts[2] in 2024, stopping bad actors before they could gain access to sensitive load data, payments, or freight.

[1] Verisk 2024 Supply Chain Risk Trends Analysis
[2] Highway 2024 Freight Fraud Trends

Top Attack Vectors in 2024

Identity Theft

Fraudsters impersonating legitimate carriers to gain access to broker loads.

Double Brokering

Illegitimate carrier transfers leading to non-payment and cargo loss.

Change in Ownership

Scammers buying old MC’s from previously legitimate companies

FMCSA Contact Manipulation

Unauthorized email and phone changes used to hijack legitimate carrier accounts.

Critical Insights from 2024

9,829 carrier users from **75 countries** attempted to access Highway from outside North America.

109,138

FMCSA contact changes detected—1,963 confirmed as fraudulent by carriers.

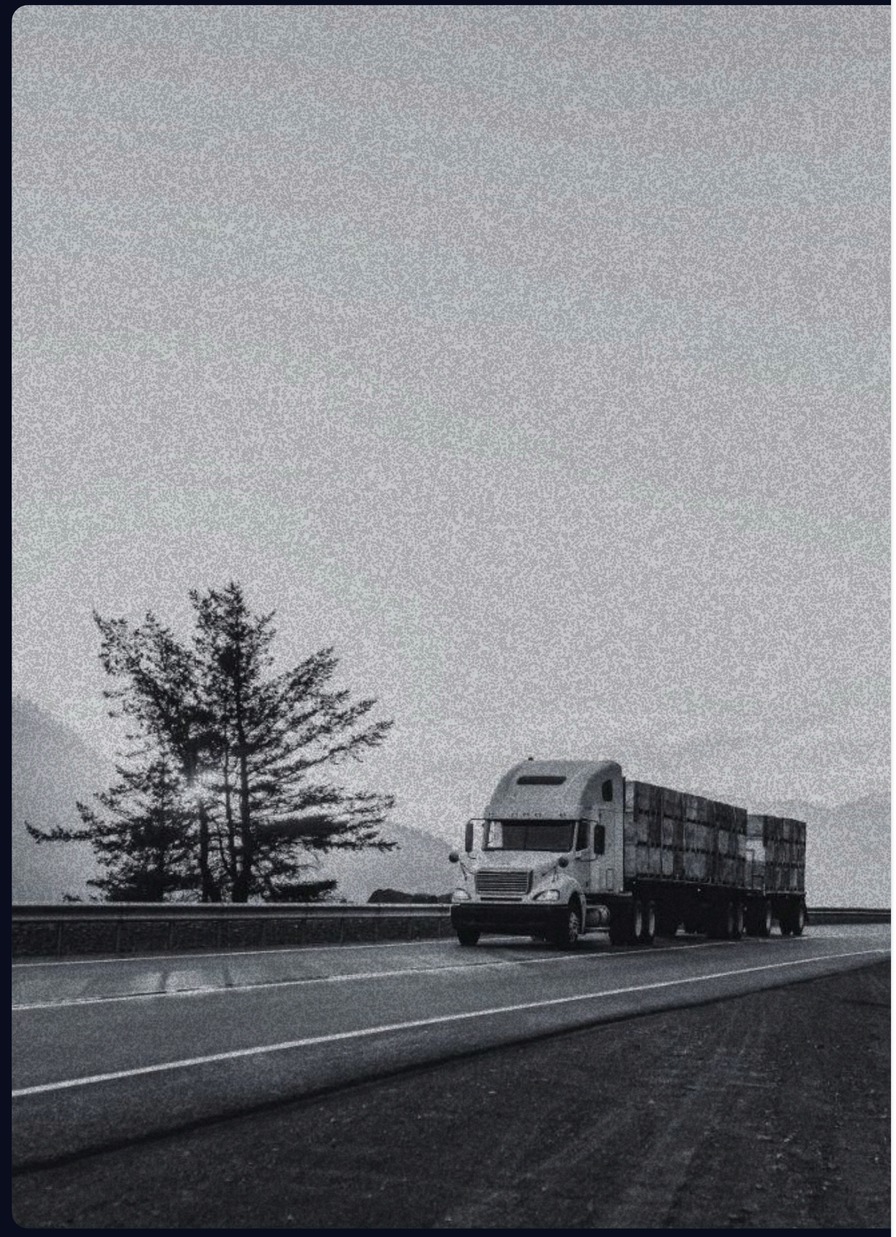
9,000+

fraudulent/spoofed phone calls blocked in Q4 2024 alone.

“

Bad actors treat **freight fraud** like a full-time job — and they've expanded their playbook. If brokers aren't adapting their defenses, they're exposing their customers, carriers, and freight to unnecessary risk. It's frustrating to see stolen loads that could have been avoided with **the right protection** in place.

Michael Grace
VP of Customer Risk Management, Highway

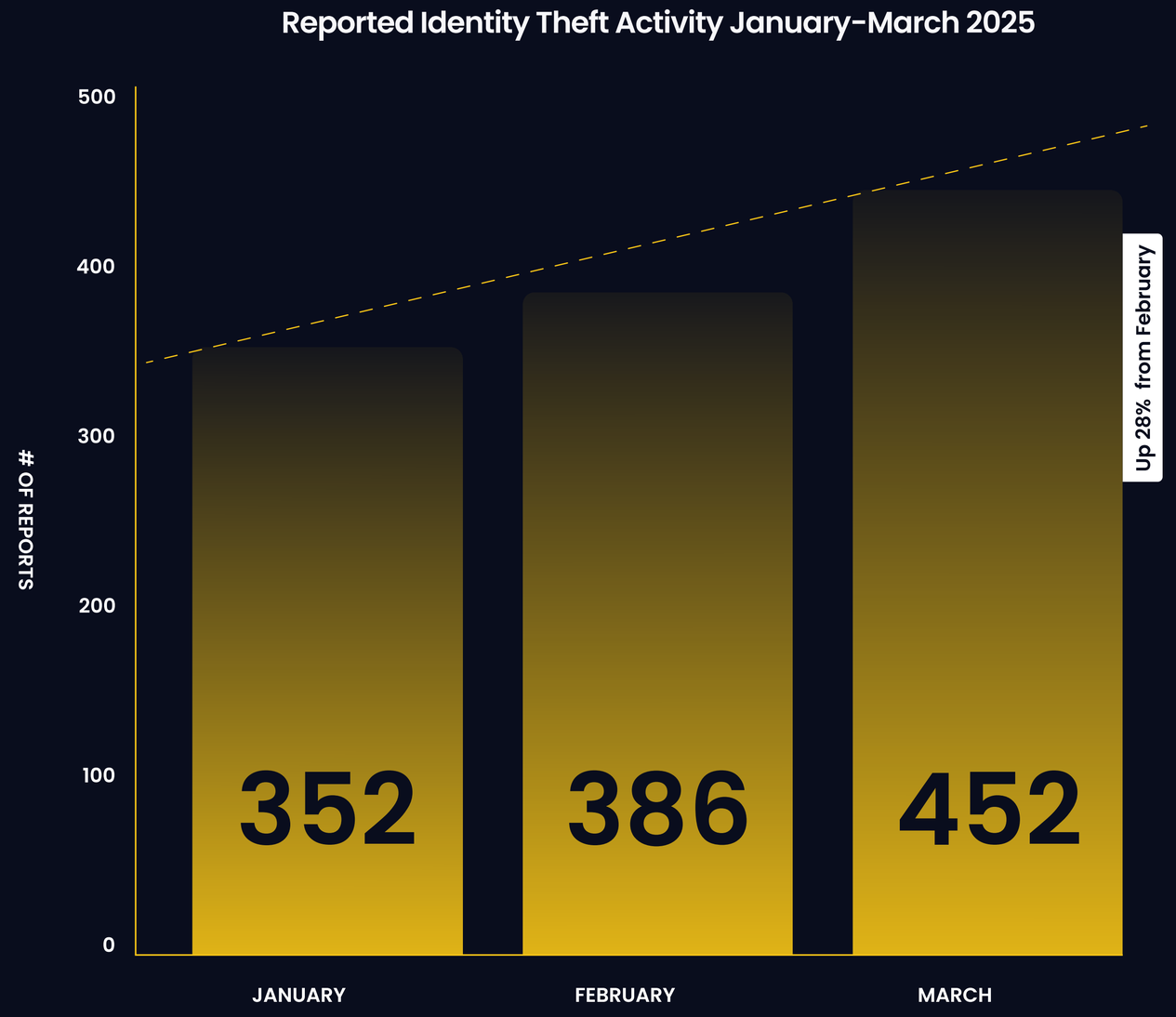


Q1 2025

Fraud Snapshot

Fraud remains an evolving challenge. In the first quarter of 2025, Highway has observed a steady rise in impersonation attempts, unauthorized contact changes, and bad actors attempting to gain access to broker networks.

Highway's proactive approach — rooted in identity verification and real-time monitoring — continues to help brokers stay ahead of these threats.



Q1 2025 Freight Fraud Trends

561

carrier users from 42 countries

attempted to log into Highway from outside North America

Top Countries

India | Moldova | Pakistan

352,134

Fraudulent Inbound Emails Blocked

406

Unauthorized FMCSA Contact Changes

30,921

Fraudulent and Spoofed Phone Calls Blocked

1,190

Fraud-Related Identity Alerts Reported

Based of Highway App, Inc. data from January - March 2025

Freight Fraud Index

How Fraudsters Are Operating Today

Freight fraud is increasing rapidly—and identity theft is leading the charge.

Bad actors are:

- Posing as legitimate carriers using stolen credentials
- Intercepting rate cons and tenders through compromised email accounts
- Using spoofed numbers and hijacked inboxes to gain trust
- Hauling loads under false pretenses—then vanishing

These aren't hypothetical threats. They're happening every day. Highway's Carrier Identity® Engine is designed to catch fraud at the source—before it reaches your inbox or phone.

Let's breakdown the three fraud vectors that spiked in Q1 2025.

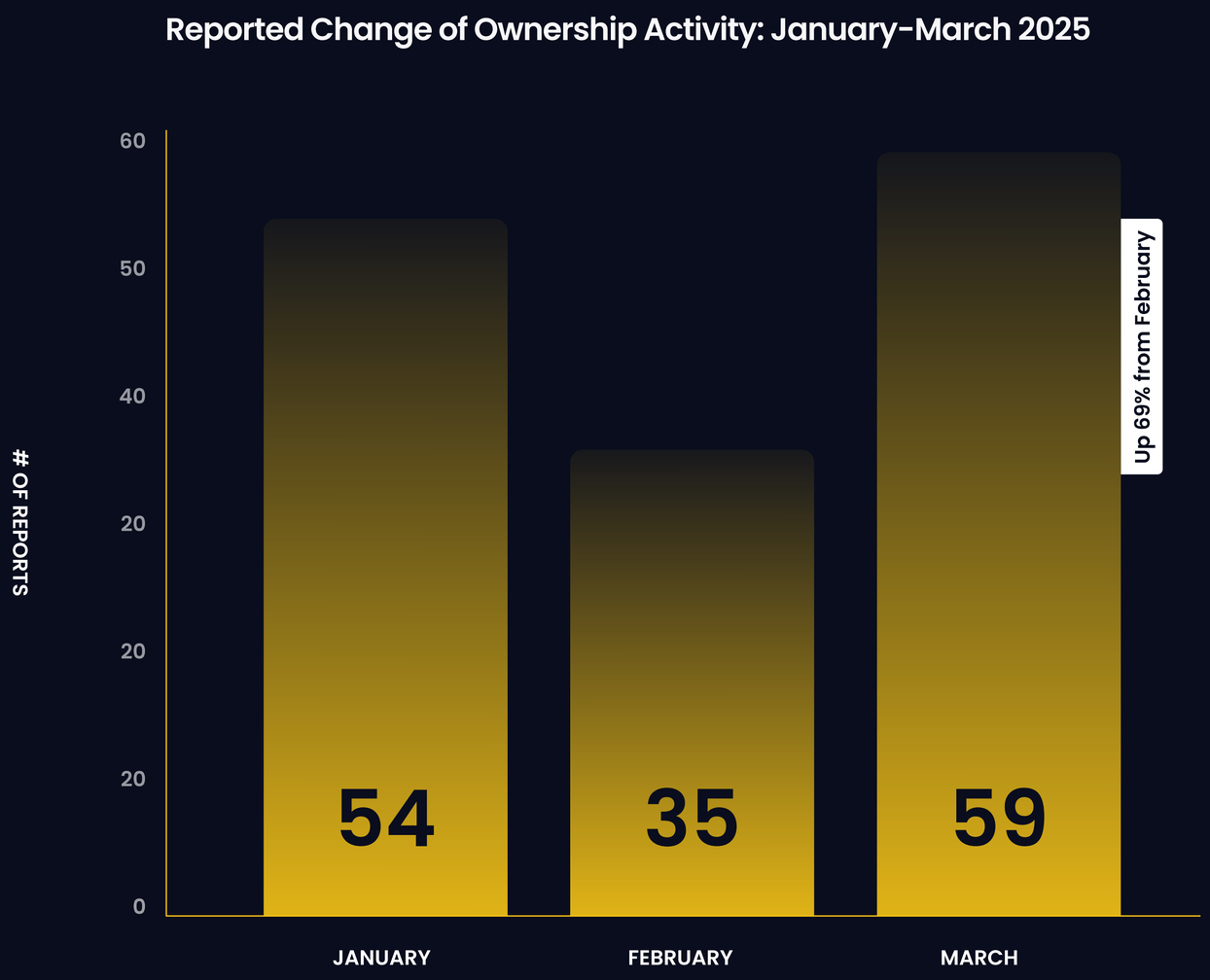
1 Sold MCs & Ownership Changes

Sold MC fraud occurs when bad actors acquire an existing, legitimate carrier's MC (Motor Carrier) number — either through an actual purchase, coercion, or deception — and then exploit that identity to commit fraud.

They often buy the MC or convince a carrier they are selling the whole business (email logins, ELD accounts, phone numbers), making brokers believe operations are unchanged.

Once bad actors gain control of the MC number, they:

1. Retain the carrier's existing broker relationships.
2. Use legitimate logins, contact information, and systems access.
3. Operate undetected for weeks or months — hauling freight, building trust, gathering intelligence.
4. Execute strategic theft — stealing high-value freight or payments — before disappearing or shutting down the MC.



Q1 2025 Trend

Surge in Ownership Changes

In the first three months of 2025, Highway tracked **148 reported cases** of change-in-ownership fraud — a pattern consistent with sold MC schemes. March saw a **69% increase** over February, indicating a surge in MC acquisitions being used as fraud fronts to steal freight, making them a critical surface area for brokers to monitor.

Hidden Threats

RED FLAGS BEHIND CHANGE OF OWNERSHIP

Already active with multiple brokers
New contact attempts to book loads under a carrier that's already established

Inactive for 2-6 months
Broker hasn't worked with this carrier recently

Insurance changes suddenly
New producer, VINs, and underwriters not listed before

Matching names, different contact info
Two users share a name but use different phones emails

Secretary of State update
Ownership or business name changes (if recorded)

"Ownership changes are usually the toughest to detect especially when there are no recorded changes. While we are actively working on additional measures to detect these transactions these are the red flags we see today:"

MICHAEL GRACE | VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

2

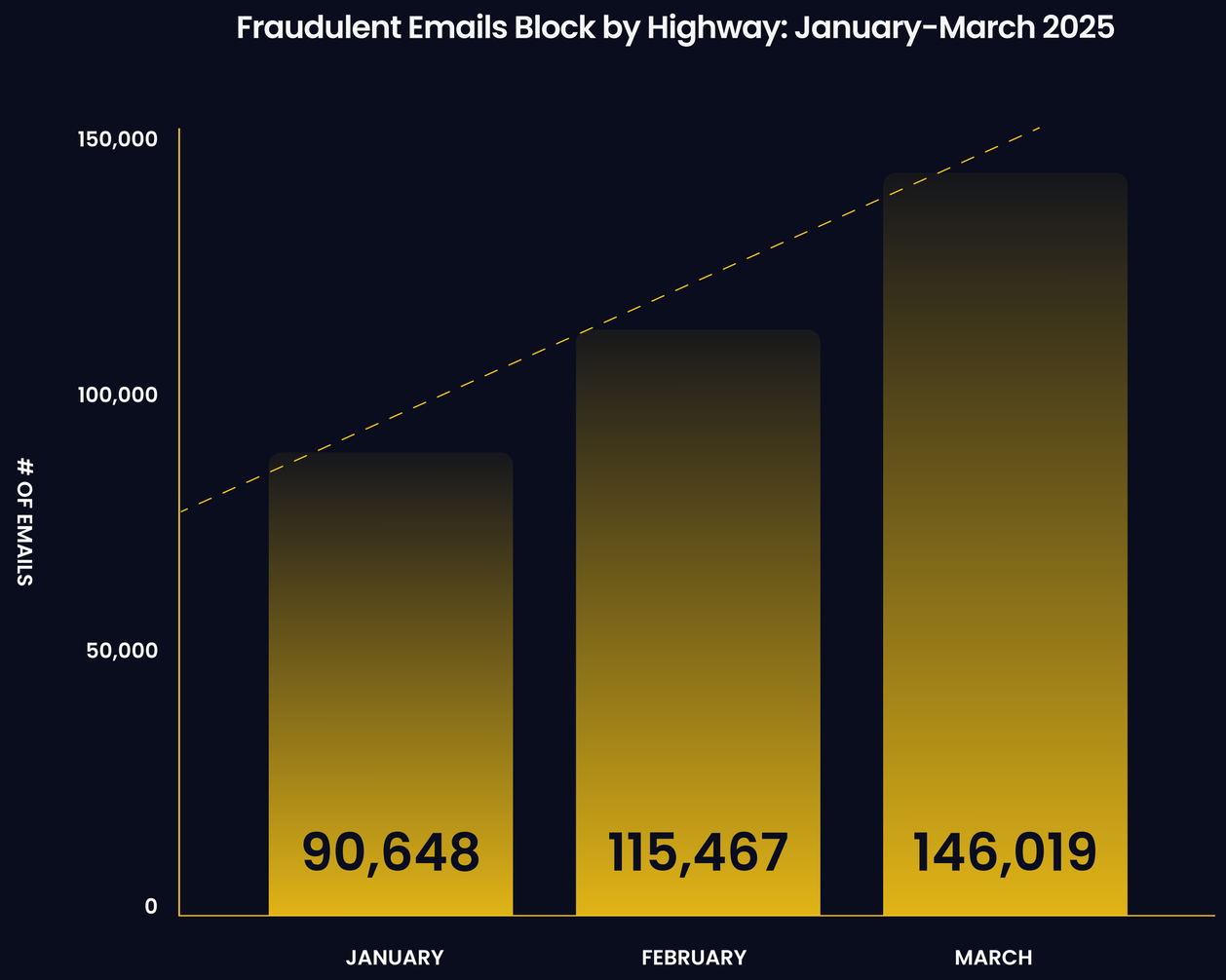
Compromised Inboxes & Email Phishing

Inbox compromise occurs when a bad actor gains unauthorized access to a legitimate carrier's email account, often through phishing links or credential harvesting from fake login pages (e.g., cloned load board portals). Once inside, they monitor conversations, impersonate the real carrier, and hijack load confirmations or payment instructions.

These attackers:

- Monitor and intercept broker communications without detection.
- Impersonate legitimate carriers using the compromised domain to hijack rate confirmations, reroute payments, or steal freight.
- Create operational confusion through conflicting instructions and last-minute changes — a tactic used to mask theft in progress.

To further mask their fraud, scammers either send poorly written, error-ridden emails or leverage AI-generated responses that are overly polished —both red flags brokers should watch for.



Q1 2025 Trend

Phishing Becomes the Front Door

Highway blocked **352,134 fraudulent inbound emails in Q1 2025**, with phishing attempts **increasing 27%** in February and another **26% in March.** This sustained growth reflects the expanding use of spoofed domains and fake login portals to gain inbox access — enabling fraudsters to impersonate carriers, intercept load details, and hijack transactions midstream.

Expert Insight

THINGS TO WATCH OUT FOR

Never trust email alone, even if it looks verified. Always **place an outbound call** using a verified phone number to confirm identity.

Watch for **communication tone red flags** like overly polished or obviously auto-generated responses that feel "off."

Avoid sending sensitive load details through vulnerable email attachments. Ensure rate cons are only accessible through authenticated, carrier-verified portals.

“This is why Highway released Secure Rate Con Delivery. Emailing rate confirmations is no longer safe. Let Highway deliver your rate confirmations for you via Secure Rate Con Delivery so you never have to deal with the “compromised email” excuse again.”

MICHAEL GRACE | VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

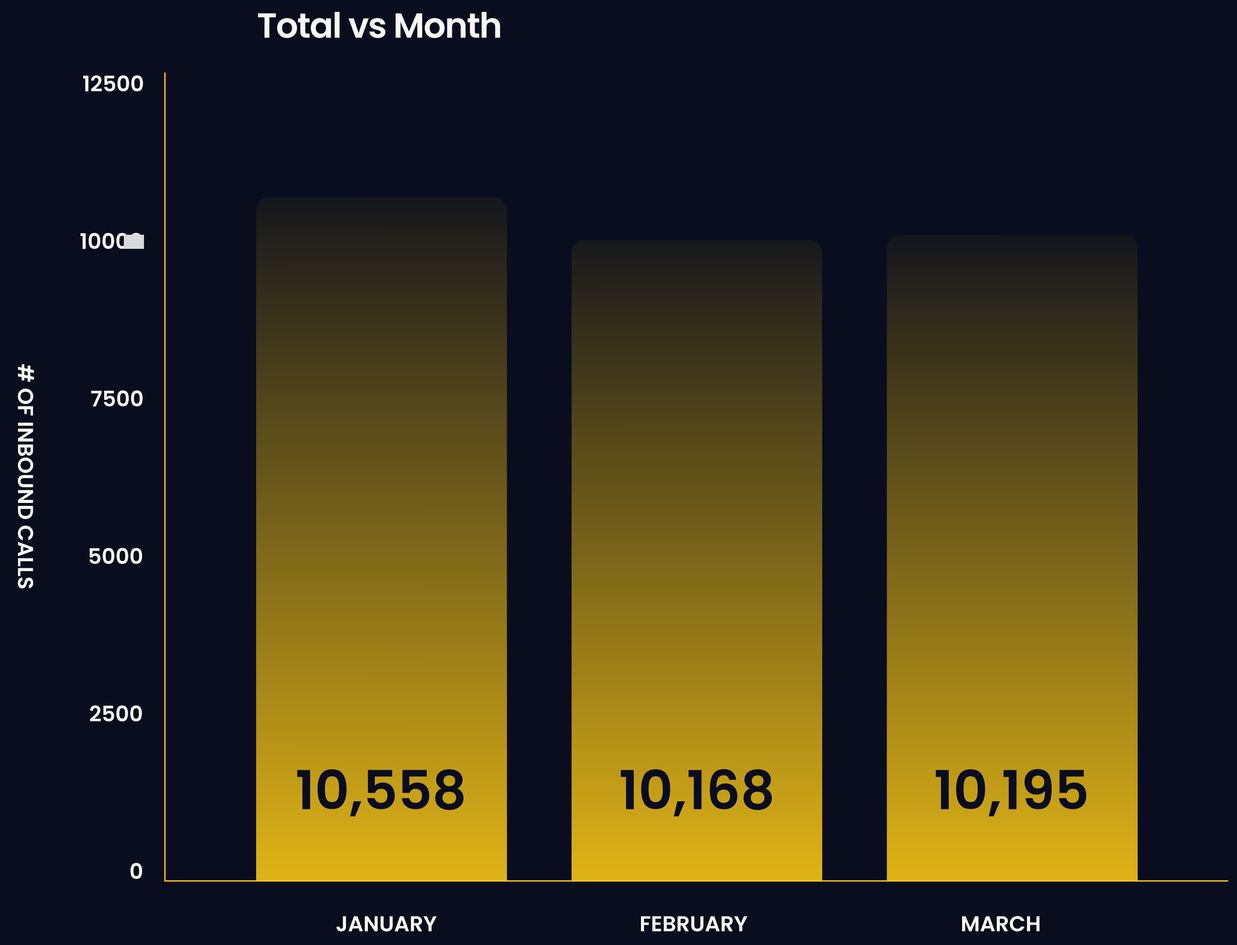
3

Phone Spoofing & Fraudulent Caller ID

Phone spoofing is a tactic where fraudsters manipulate the caller ID to impersonate a legitimate carrier or dispatcher. When brokers receive an inbound call from what appears to be a trusted number — often one already tied to a carrier in their system — they're more likely to bypass normal verification steps and move quickly to book the load.

How the Phone Spoofing Works:

1. A broker receives a call from a number that appears legitimate. Trusting the caller ID, they proceed without further verification — the exact gap spoofed numbers are designed to exploit.
2. The fraudster references a compromised email to build credibility, prompting the broker to send the rate confirmation without confirming the phone number.
3. In the rush to cover the load, verification is skipped. With the rate con in hand, the fraudster takes the freight and disappears.



Q1 2025 Trend

Spoofed Numbers Enabling Stolen Loads

Highway flagged **30,921 spoofed phone numbers** in Q1 2025. Many of these calls were part of stolen load incidents involving compromised email addresses and reused driver phone numbers. In one confirmed case, a phone number used to impersonate a dispatcher had been flagged for fraud **nine times prior** — but the broker failed to verify it before sending the rate confirmation.

Cut Off The Call

STOPPING FRAUD BEFORE IT STARTS

Implement phone number **validation technology** to authenticate incoming calls and verify they come from trusted carriers.

Before providing load details, payment terms, or contracts **always verify caller identity** through a secondary method, like email, system checks, or a callback.

Educate team members on common tactics and equip them with **tools to spot red flags**, preventing fraud before sensitive information is shared.

"Highway's solution for this is Highway for VoIP where we integrate with your VoIP provider to re-route spoofed, fraudulent and high risk phone numbers out of your network before they have a chance to get a load from an unsuspecting broker trying to cover freight."

MICHAEL GRACE | VP OF CUSTOMER RISK MANAGEMENT, HIGHWAY

Q2 2025 Fraud Forecast

Produce Season Risks & Threats

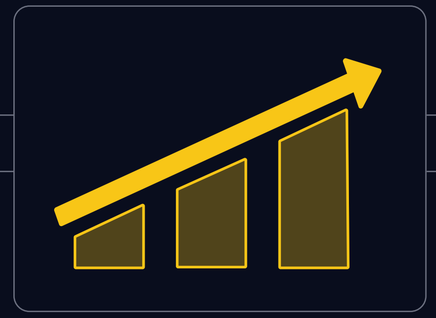
As we look ahead into Q2, Highway's VP of Customer Risk Management, Michael Grace, foresees fraud to continue evolving especially in spoofed communications—by email or phone—and a surge in load theft attempts as we head into spring and summer produce seasons.

"As the tools for fraud become more sophisticated, so must our methods of prevention and response." The continuance of proactive measures and technology adoption as essential for staying ahead of fraud trends.

What to Watch Out for in Q2 of 2025

Increase in Spoofed Communications

A common tactic can involve bad actors calling brokers to get them off the computer screen and away from the true data. By spoofing their phone number or legitimate carrier information, such as an email address, they attempt to convince the broker that they are who they say they are. To further manipulate the situation, they may even provide fake FMCSA contact details, convincing brokers that the carrier is properly registered. This leads brokers to let their guard down, potentially opening the door to fraud.



Surge in Load Theft Attempts

Load theft is becoming more sophisticated, with fraudsters exploiting weaknesses in verification processes to steal shipments. These bad actors often combine multiple tactics—such as identity theft, buying old MC's, FMCSA contact manipulation, and spoofed communications—to deceive brokers and hijack freight.

2025 Q1 Freight Fraud Index

KEY TAKEAWAYS

What the Data Reveals

The Freight Fraud Index confirms that fraud and strategic cargo theft are on the rise, with identity theft, false pickups, sold MCs, double brokering, and FMCSA contact manipulation remaining widespread. In Q1 2025, fraudsters deployed more sophisticated tactics—compromising carrier email accounts and spoofing caller IDs—to deceive brokers and infiltrate networks. Staying vigilant requires more than reactive checks—it demands purpose-built tools and proactive identity controls.

Highway's Role in Preventing Fraud

Highway blocked over 400,000 fraud attempts in the first quarter of 2025, underscoring the scale and sophistication of today's identity-driven attacks. Brokers using Highway move beyond basic vetting—building custom classifications, applying their own rules, and continuously monitor carrier identity. From detecting risk signals across email and phone to protecting every load with Load Lock, Highway equips teams to adapt in real time. As fraud tactics evolve, Highway provides the intelligence and infrastructure to stay ahead—proactively, precisely, and at scale.

To learn more about Highway's Carrier Identity® Solution for Fraud Prevention, book a demo here.

highway.com