HIGHWAY

Q3 2026

FREIGHT FRAUD INDEX REPORT

Real credentials, wrong hands

The credentials behind this quarter’s fraud were real. What changed was who controlled them. Checks that verified identity before load details were shared helped stop theft.

FROM THE EDITOR

Who’s on the other end



DEMI RAMON
Vice President of Risk, Highway

Verification starts with identity. Protecting a load requires staying alert to what changes next.

Highway's mission is to help answer a fundamental question: Is this carrier who they say they are? This quarter's activity reinforced another: Is the carrier you vetted still the one hauling your load?

Compromised carrier inboxes and other cyber-related thefts were central to that challenge. Criminals used legitimate email accounts and established relationships to make fraudulent requests look routine. Changes in ownership also created another opportunity to operate behind a familiar authority. A carrier's history could remain recognizable even as the people controlling its communications or operations changed.

The relationships you've built remain valuable, but trust requires ongoing verification. Well-trained teams, consistent processes, and the right tools help brokers identify changes and confirm that the carrier they selected is the one handling their freight. Ongoing verification turns trusted relationships into safer loads.

This report reflects activity reported to Highway, rather than the industry as a whole.



THE FINDING

The fraud reported to Highway this quarter highlighted the need for verification throughout a carrier relationship.

Compromised email accounts and changes in ownership allowed bad actors to operate under legitimate carrier identities, exploiting trust established before they became involved. Verification at onboarding remained important, but could not account for every subsequent change in who controlled the business or its communications.

Secure Rate Confirmation Delivery (SRCD) helped address that exposure. Greater adoption, combined with additional identity verification before access to sensitive load information, helped limit opportunities for compromised inboxes to lead to successful thefts. These findings reinforce the value of verifying the person accessing a rate confirmation when that information is released.

Several risk indicators increased during the quarter. Identity Alerts increased 5.4% and change-of-ownership reports increased 111% this quarter. These measures provide context for the activity Highway detected and received reports about; they should not be interpreted as equivalent increases in confirmed theft.

Over the same period, stolen loads reported to Highway declined 28.1%, marking the second consecutive quarterly decrease. That decline describes the reports received by Highway, rather than an industry-wide reduction in cargo theft. Customer growth and reporting participation also affect the volume captured in this Index.

The following three findings examine how bad actors exploited carrier identities, where verification helped interrupt those efforts, and where exposure remained.

THE QUARTER IN CONTEXT

Nobody has defined *careful selection of carriers.*

A broker can be sued for the carrier it chose, and no state statute or regulation clearly defines careful selection. Four Q3 events—and a preceding Supreme Court decision—highlighted the potential vulnerabilities of those who stand in the gap.

May 14

The Supreme Court decided Montgomery v. Caribe Transport II unanimously: A negligent-selection claim against a broker is not barred by federal law.[1] What careful means is now for state courts, one case at a time.

July 23

A Dallas County jury returned a $604 million verdict over a fatal crash and assigned about two-thirds of it to the broker. The verdict may be appealed.[2]

August 4

The Fifth Circuit allowed a negligent-selection claim to proceed against a broker, even though the carrier was selected through a chain of subcontractors rather than directly by the broker.[3]

September

Until further notice, the FMCSA stopped deactivating USDOT numbers for missed biennial updates during its move to Motus. The record a broker checks can be older than it looks.[4]

September 29

A Los Angeles jury convicted two men who bought established trucking companies — one for about $22,000 — booked loads through brokers, and never delivered. Every credential was real.[5]

[1] Montgomery v. Caribe Transport II, LLC, U.S. Supreme Court, May 14, 2026. [2] Dallas County District Court, jury verdict, July 23, 2026; figures from the broker's Form 8-K. [3] U.S. Court of Appeals for the Fifth Circuit, No. 25-40012, Aug. 4, 2026. [4] FMCSA notice on biennial-update enforcement during the Motus transition, September 2026. [5] U.S. Attorney's Office, Central District of California, press release, Sept. 29, 2026; also cited on page 10.

Q3 2026 AT A GLANCE

More attempts, fewer thefts than in Q2

28.1% Reported stolen loads, change from Q2 2026.

The second quarterly decline in a row.

90.3% Fraudulent and spoofed calls blocked, change from Q3 2025.

119,022 this quarter. The fastest-growing measure with a year-over-year comparison.

THE QUARTER IN NUMBERS

Reported stolen loads fell 28.1% from the second quarter.

Third quarter was quieter than the second quarter based on normalized data.

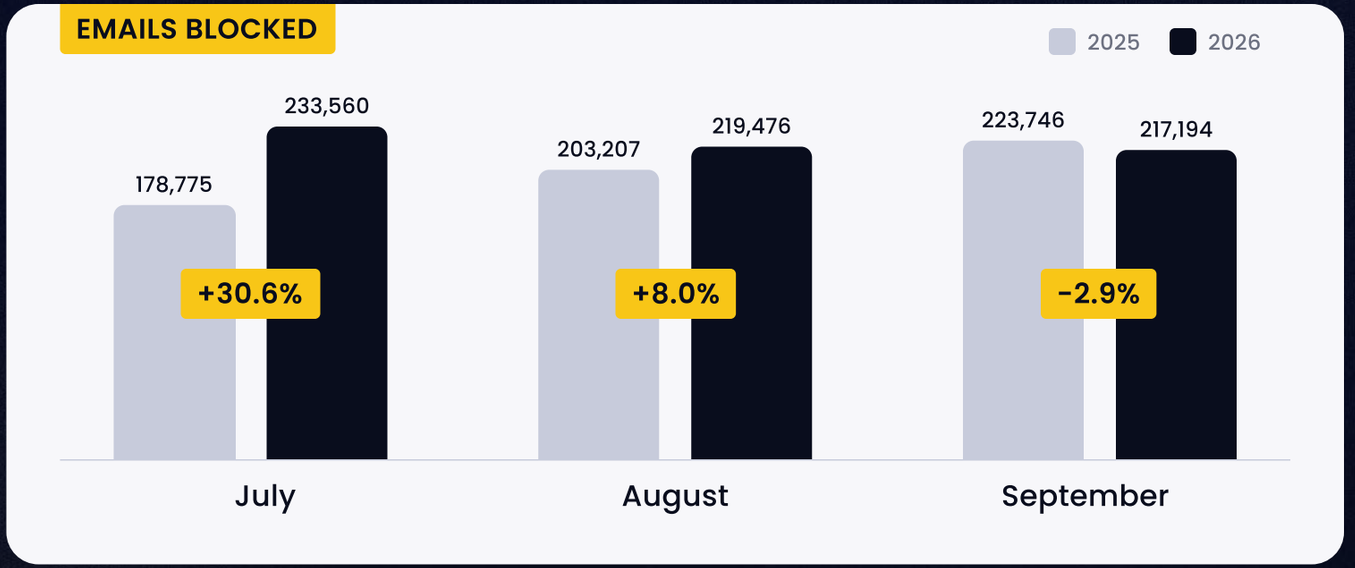
The figures provide a closer look at how key freight fraud indicators shifted throughout the quarter, highlighting changes in reported activity and emerging risk trends compared to previous periods.

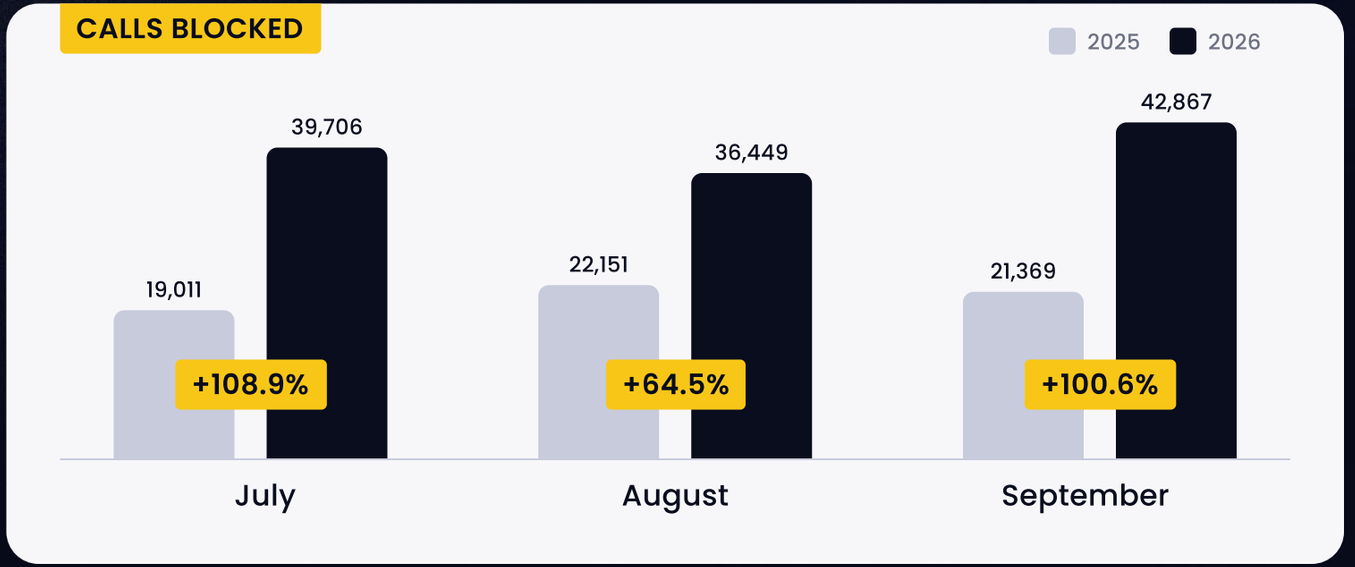
METRIC	Q3 2026	vs. Q2 2026	vs. Q3 2025
Stolen loads reported	184	-28.1%	+8.2%
Fraudulent inbound emails blocked	670,230	-14.5%	+10.6%
Fraudulent and spoofed calls blocked	119,022	+8.2%	+90.3%
Unauthorized FMCSA contact changes	15,491	+12.7%	-
Change-of-ownership reports	518	+111.4%	+12.4%

BLOCKED EMAILS AND CALLS BY MONTH

Calls blocked ran 64.5% to 108.9% above last year, every month.

Emails blocked ran ahead in July and August, fell 2.9% below in September, and declined each month within the quarter. One quarter is too short to call that a move from the inbox to the phone. Both counts grow with the network, so read the months for shape, not size.



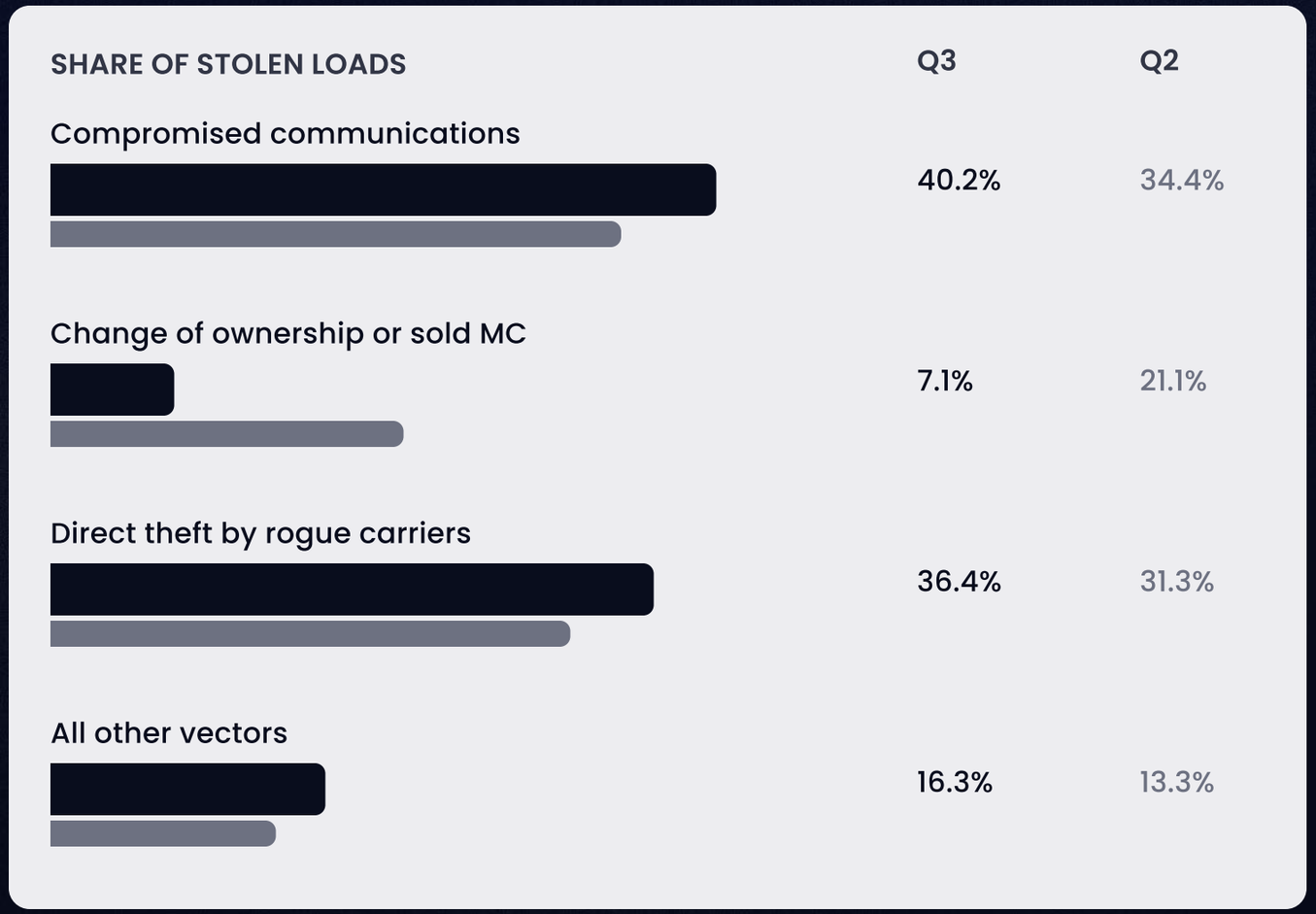


WHERE THE THEFTS CAME FROM

Compromised communications led again.

Following the trend we observed in Q2, compromised communications were the most common way bad actors entered broker networks. This time last year, direct theft was the leading cause of thefts reported to Highway.

Three attack vectors accounted for more than 80% of stolen loads reported to Highway this quarter. The findings examine these methods, including how bad actors exploited legitimate carrier identities and credentials to gain access to freight.



HOT SPOTS

California led the hot-spot states again

California remained the most common pickup state for stolen loads reported to Highway, accounting for nearly half of the total, with New Jersey ranking second. Direct theft was also concentrated among carriers domiciled in California—a separate measure based on the carrier's home state rather than the load's pickup location.

HOT-SPOT STATES, BY PICKUP

1. **California**
2. New Jersey
3. Texas

TOP TARGETED COMMODITIES

1. **General merchandise**
2. Electronics
3. Bulk commodities

TOP COUNTRIES, BLOCKED SIGN-INS

1. **Colombia**
2. India
3. Philippines

Highway blocks sign-in attempts that appear to originate outside a user's home country. Because bad actors can disguise their connection's origin, the country recorded for an attempt may not reflect their physical location.

FINDINGS / A

The target was the ownership check. Now it's the attestation.

Thefts reported to Highway involving a change in ownership declined this quarter, even as reports of ownership changes increased. Highway's ownership attestation process added an additional step when potential changes were detected, helping identify risks that a carrier's established history alone would not reveal.

Authorities are still for sale, as the Los Angeles verdict on page 4 showed.[1] With Highway's checks in place at transfer, attacks have shifted to the attestation itself. In some instances, bad actors have sought to implicate sellers in their schemes. Some offered sellers compensation to submit false attestations, despite the additional legal exposure for those sellers.



What changed since Q2

The attack moved from the sale to the signature.

What didn't change since Q2

Inherited trust still draws the attempt, whether it's a sold MC or a carrier you've used for years.

[1] U.S. Attorney's Office, Central District of California, press release on the verdict in United States v. Singh, Sept. 29, 2026; republished at irs.gov/node/166056.

FINDINGS / B

Direct theft took a larger share. License-related risk remained a concern.

The number of stolen loads attributed to direct theft fell 16% from Q2. Compared with a 28% decline across all stolen loads reported to Highway. As a result, direct theft's share increased to 36.4% of overall reported theft volume.

In these cases, the carrier entrusted with the freight carried out the theft. An established operating history, trucks, and an apparently routine pickup could make the transaction look legitimate until the load failed to arrive. Some carriers took several loads within a few days, increasing the potential loss before brokers recognized the pattern.

The quarter also continued a pattern Highway has tracked since Q4 2025: direct theft involving carriers whose drivers held non-domiciled or limited-term CDLs. That recurring association reinforces the importance of reviewing the people operating under a carrier's authority alongside the carrier's business history.

FROM THE RISK DESK

The capacity trade-off is smaller than you think.

Brokers often leave non-domiciled and limited-term CDL rules disabled to preserve carrier capacity. But when configured for the highest-risk states and a fixed look-back period, enabling the rule reduces available capacity by approximately 7%. Ask your account team to measure the impact on your network.

87%

of direct theft events reported to Highway over the last 90 days involved carriers with a Highway user whose identity verification history included a non-domiciled or limited-term CDL designation

FINDINGS / C

Protecting load information through verified access

Compromised communications remained the most common theft vector reported to Highway this quarter. When a bad actor gains access to a carrier's inbox, an email exchange can appear legitimate while exposing sensitive load information to someone unauthorized to receive it. Rate confirmations sent as attachments can be accessed or forwarded without the broker knowing who ultimately received them.

Secure Rate Confirmation Delivery (SRCD) helps address this risk by requiring authenticated access to load documents and recording which carrier user accessed and accepted them. This provides an opportunity to verify the recipient before releasing information that could be used to execute a theft.

The quarter's findings reinforce the importance of protecting load information throughout the transaction. Verifying a carrier at onboarding establishes the relationship; verifying access to a rate confirmation helps confirm who is acting on that relationship when a load is tendered.

FROM THE RISK DESK

Secure Rate Confirmation Delivery moves rate confirmation delivery and acceptance into Highway, adding an audit trail beyond the email exchange.

This helps reduce the risk of a compromised carrier inbox being used to obtain load details and impersonate a trusted carrier. That protection depends on keeping the process in-platform rather than reverting to emailed attachments that can be intercepted by a bad actor.

INTELLIGENCE WATCH

Chameleon carriers

Chameleon carriers close one authority and reopen under another with the same trucks and people. The signal is reuse: the same VIN on insurance certificates for more than one carrier, or the same identity document behind more than one account.

This data reflects a signal, not fraud. Affiliated companies, leased equipment, and clerical error all produce shared VINs and documents, and no single signal is evidence of fraud. This is the first quarter counted on its own, so it doesn't compare with the last Index's first-half figures.

VINS ON INSURANCE CERTIFICATES

22,020

VINs appeared on insurance certificates for more than one carrier

975 of those appeared on certificates for three or more carriers

104 of those appeared on certificates for five or more carriers

15 carriers shared the single most-used VIN

IDENTITY DOCUMENTS

5,336 identity documents were tied to more than one Highway user account

746 of those spanned more than one carrier authority

FORECAST

Three calls for Q4, and the sign that grades each one

1

Holiday volume will bring more theft.

Reduced carrier availability can create openings for bad actors to exploit the urgency to cover loads.

SIGN TO WATCH

Reported stolen loads increase in Q4 compared with Q3.

2

Compromised emails remain the most common threat.

Bad actors exploited gaps in email security and used urgency to pressure recipients into acting before verifying a request

SIGN TO WATCH

Compromised communications remain the largest share of stolen loads reported in Q4.

3

The Highway Certified Network is growing

Insurance agents and ELD providers will bring shared accountability and enforceable standards to brokered freight.

SIGN TO WATCH

Look for badges at the top of the carrier profile to see whether the carrier works with Highway Certified partners.

FIELD GUIDE

What to watch for and what to do.

Red Flags	Best Practices
Rate confirmations are sent as attachments without confirming who accesses the load information.	Require a verified, authorized carrier user to authenticate before accessing rate confirmations.
An inbound caller is trusted based on a familiar phone number or voice.	Verify sensitive requests by making outbound calls to the carrier's verified contact information.
An established carrier relationship replaces verification of the people handling the current load.	Confirm that the person arranging the load is authorized to represent the carrier, and verify the assigned driver's contact information before pickup.
After-hours exceptions proceed without a clear review or escalation process.	Assign responsibility for reviewing exceptions and establish escalation coverage for nights and weekends.

FROM THE RISK DESK

Use the control list on page 18 to document which protections your organization uses, who owns each one, and how exceptions are reviewed.

BEFORE THE NEXT QUARTER

Define how exceptions are handled.

A carrier selection standard is only effective when teams apply it consistently, including when a load needs to move after hours or a familiar contact requests an exception. Those situations need clear expectations for verification, approval, and escalation.

Technology providers offer tools and documentation to support your carrier selection standard. Your organization determines how those protections fit into daily operations and who is responsible for using them.

Document which checks are required, who can approve an exception, and what information must support that decision. Establish coverage for nights and weekends so employees know where to turn when a carrier cannot meet the requirements.

Train teams on those expectations and reinforce them through accountability. Recognize employees who follow the process and raise concerns, address missed steps through coaching, and apply consistent consequences when required checks are repeatedly or deliberately bypassed.

That’s the quarter. Back to the board. Before the next load moves, verify who holds the credentials today.

Use these findings to review your verification practices, address process gaps, and prepare your team to handle exceptions. Share the report with the people responsible for booking loads and verifying carriers, including those covering nights and weekends.

If you discover a theft or suspicious activity, report it promptly. Your report helps Highway identify patterns, investigate potential threats, and alert other brokers to risks they may also face.

LET’S TALK

Report fraud or suspicious activity
reportfraud@highway.com

Review your network’s activity and use of controls
Contact your account team or connect with us at highway.com.

Controls in this report

The controls in this report combine technology with the processes your team follows every day. Highway provides tools to support verification and monitoring. Your organization sets the requirements, assigns responsibility, and ensures those controls are applied consistently.

CONTROL	WHAT IT ASKS OF YOUR TEAM	WHERE HIGHWAY HELPS
A fresh check at every change of ownership	Reassess the carrier's ownership and authorized contacts. Review applicable alerts, rule results, and required verification before tendering another load. Treat an attestation as part of that review.	Connect supports ownership attestations and displays Identity Alerts and rule results to help teams evaluate potential or confirmed ownership changes.
A verified, authorized person on every rate confirmation	Use secure delivery that requires a verified, authorized carrier user to authenticate before accessing load information. Establish an escalation process when verification cannot be completed.	Secure Rate Confirmation Delivery, part of Load Lock, delivers rate confirmations through authenticated access, reducing reliance on attachments sent directly to an inbox.
License screening before tender	Configure the ND/LT rule's state and look-back criteria for your network. Review rule results before tendering a load and define who may approve an exception.	Connect evaluates ID information submitted by carrier users against the configured ND/LT criteria and reflects the result in the carrier's rule status.
The driver's number, checked before pickup	Provide the assigned driver's phone number with each load. Investigate and resolve related fraud alerts before pickup.	Load Lock, also included in Load Lock+, checks submitted driver phone numbers for associations with reported fraud and generates alerts for review. Connect allows users to search phone numbers and email addresses in the portal to determine whether they have been flagged for fraudulent activity.
An owner for every exception	Define who can approve exceptions, what evidence is required, and how concerns are escalated during nights and weekends. Train employees and reinforce consistent compliance.	Load Lock supports documenting alert reviews and decisions. Your organization establishes approval authority, escalation coverage, and accountability.


HIGHWAY
highway.com