State of Fraud in the Industry

April 2025 Report (2nd Edition)

Report findings reveal extent of the threat, financial impact, and critical steps the industry must take to protect itself

Introduction

The logistics and transportation industry continues to battle a wave of increasingly complex and coordinated fraud schemes. From unlawful brokering to identity theft and cargo theft, third-party logistics companies are being targeted at unprecedented levels. The threat is not only persistent—it's evolving.

Findings from this latest six-month update to the TIA Fraud Report confirm what many members already feel: unlawful brokering remains the most prevalent form of fraud, and fraudsters are using more sophisticated methods to spoof identities, manipulate documentation, and infiltrate systems. While prevention efforts have grown stronger, the fraud landscape has grown more aggressive in return.

This report offers a comprehensive view of the current fraud climate, and explores the financial and operational impact on brokers, highlights the commodities and regions most affected, and surfaces member-driven solutions that are helping the industry fight back. As the trusted voice of third-party logistics, TIA remains committed to equipping members with the tools, data, and advocacy needed to protect their businesses and the broader supply chain.

Purpose of the Report

The logistics industry continues to face unprecedented levels of fraudulent activity, with new schemes emerging just as quickly as countermeasures are developed. This updated report—TIA's second edition in an ongoing series—aims to deepen our understanding of the evolving fraud landscape. It draws from two core data sources: a member survey conducted in early 2025 and six months of fraud reports submitted through TIA's Watchdog platform.

By combining real-time feedback from 3PL professionals with industry-wide incident data, this report provides a clearer picture of how fraud is impacting businesses, where it's happening, and what tactics are being used. It's designed to arm logistics professionals with timely insights and practical strategies to protect their operations, customers, and the broader supply chain.

As fraudsters become more sophisticated, the industry must respond with equal urgency and coordination. This report offers a snapshot of both the challenges and the resilience shaping the current response—and the leadership role TIA continues to play in moving the industry forward.

The Current Landscape of Fraud in Logistics

Overview of Fraud Types

Cargo Theft: This remains the most prevalent and costly form of fraud affecting the logistics sector. According to the National Insurance Crime Bureau, cargo theft is now costing the industry up to **$35 billion annually**, with a **1,500% increase in incidents since 2021.** This surge is not only straining operations but driving up costs across the entire supply chain, ultimately impacting consumers. In this reporting period alone, 96% of TIA survey respondents reported dedicating time each quarter to managing fraud-related incidents—many tied directly to cargo theft.

Financial Theft: This includes financial schemes like unlawful brokerage and fraudulent invoicing. While cargo theft represents the largest financial losses per incident, unlawful brokerage remains the most frequently reported type of fraud. In the latest TIA survey, **34% of respondents** identified unlawful brokering as the most frequent type of fraud they experienced. These schemes often involve bad actors impersonating legitimate brokers or carriers, inserting themselves into freight transactions, and diverting loads or payments. Watchdog data reflects this trend, with **402 incidents** of unlawful brokerage reported in just the past six months.

Identity Theft: Criminals frequently steal the identities of legitimate companies to impersonate them during the booking and pickup process. This tactic is used to gain access to high-value freight or falsify payment and communication records. **20% of respondents** cited identity theft as their most frequent fraud concern in this reporting cycle, while another **22%** reported experiencing email spoofing most often.

Internal Theft: Although less frequently reported than external schemes, internal fraud remains a concern for some 3PLs. This can include the unauthorized sharing of sensitive data, collusion with bad actors, or manipulation of internal systems to divert funds or freight.

Data/Information Theft: Cyber-attacks targeting emails, passwords, TMS platforms, and insurance data are becoming more sophisticated and targeted. These breaches not only compromise operations but also erode trust across the logistics chain.

NICK MADAHAR AND ANNIEPREET (ANNIE) SINGH | SHINE LOGISTICS GROUP | ELK GROVE, CA

Nick Madahar and Anniepreet (Annie) Singh from Shine Logistics thought they had vetted a reliable carrier—95/100 rating, verified insurance, and a solid track record. But they were unknowingly dealing with fraudsters who hijacked a legitimate company's identity.

"We did everything right, yet they still scammed us," Annie said. The criminals altered official details across multiple verification portals, used a leased truck under a different name, and disappeared with nearly $291,000 worth of artificial nails. By the time the real carrier realized their identity had been stolen, the load was gone—transloaded onto another truck and untraceable.

"The worst part? There's no clear way to recover from this. Fraudsters are evolving faster than enforcement, and insurers refuse to pay out," Nick added. Shine Logistics has tightened security, but their story underscores a growing crisis: supply chain fraud is outpacing industry protections.

Trends and Statistics

High-Risk Areas: The latest TIA survey confirms that fraud continues to concentrate in logistics hotspots, with **Texas (19%)** and **California (14%)** leading as the top states where incidents originated. Other notable mentions include **South Carolina (8%), Washington (8%)**, and **Virginia (7%)**—regions with major freight corridors and infrastructure, making them high-value targets for organized fraud rings.

Targeted Commodities: Criminals are still focused on stealing high-value, easy-to-resell goods. The most frequently targeted commodities in this reporting cycle were **household goods (23%), electronics and appliances (15%), frozen or refrigerated foods (9%)**, and **printed material and packaging (9%).** These trends emphasize the need for heightened security around shipments that are both valuable and difficult to trace once stolen.

Impact on Businesses: The financial toll of fraud remains staggering. While **36% of respondents** reported relatively minor losses under $5,000, over **half (53%)** experienced losses exceeding $10,000—and **22%** reported more than **$200,000 lost.**

Prevention efforts are also a significant expense. While **36%** spent under $5,000 to mitigate fraud risks, another **52%** of respondents invested **more than $10,000**—with **10%** spending over **$200,000** on technology, staff time, insurance, and training.

Time, too, is a major cost. A combined **65% of companies** reported spending **more than two hours per day** on fraud prevention each quarter, with **24% saying it's an all-day task.** Even after fraud incidents occur, **37% of respondents** said their teams spend more than two hours per day dealing with the fallout—whether in claims management, customer communications, or operational disruptions.

These numbers reinforce what many in the industry already know: fraud isn't just a threat—it's a drain on time, money, and resources. And it's affecting businesses of all sizes.

Survey Data Analysis

Prevalence and Impact of Fraud Across the Industry

Primary Target of Fraud: Truckload freight remains the primary target of fraud, with 97% of respondents identifying it as the most vulnerable mode — virtually unchanged from the September 2024 report. This consistency highlights the ongoing need for heightened security measures in full truckload operations.

Frequency of Fraud Types: Unlawful brokering scams continue to top the list of threats, cited as the most common fraud type by 34% of respondents. Spoofing followed at 22%, with identity theft close behind at 20%. Other tactics like phishing (6%), fictitious pickups (8%), and impersonation via inbound phone calls (6%) show that the threat landscape remains varied and sophisticated.

Multiple Fraud Types: Eight types of fraud were shared in the survey and respondents were asked to indicate any and all that they experienced: spoofing, unlawful brokerage scams, fictitious pickups, phishing, identity theft, email/virus, inbound phone calls, and text messages. Fraud is rarely isolated. 83% of respondents reported experiencing at least three types of fraud, 71% experienced four or more, and 7% experienced all eight types listed in the survey. This underscores a broader reality: companies aren't just managing one type of fraud—they're navigating layered, coordinated threats across multiple vectors.

VICTOR LOUIS | ONE LOGISTICS NETWORK | CINCINNATI, OH

Victor Louis experienced a highly sophisticated freight fraud scheme involving stolen aluminum shipments that were likely redirected overseas. The perpetrators used GPS location updates to make it appear as though the cargo was in transit, buying time to complete the theft. Soon after, Victor's team identified another attempt using the same fraudulent tactics and reported it. In retaliation, the criminals—posing as a legitimate, vetted carrier—held another shipment hostage and threatened Victor to remove a fraud report against their company.

A break came when a warehouse employee tipped off authorities about the stolen shipment's whereabouts. However, before the authorities could act, the fraudsters manipulated and intimidated the warehouse employees, regaining possession of the goods. Victor later uncovered international ties to Armenian and Albanian criminal networks, but law enforcement dismissed the case as a civil matter, making it nearly impossible to report.

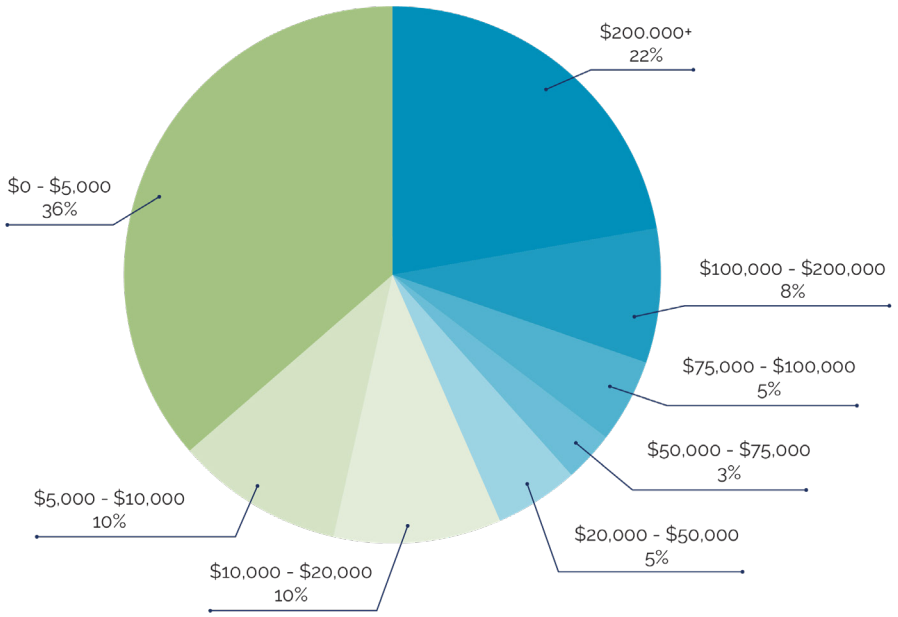
"The criminals hide in plain sight, running 'legitimate' businesses as fronts. The lack of action from law enforcement and government officials only emboldens them," Victor said. "The inaction is hurting businesses, disrupting relationships, and threatening the integrity of interstate commerce. This crisis is bigger than our industry—it's a global issue."

Financial Impact

The financial toll remains substantial.

- 22% of respondents reported losing more than $200,000 due to fraud.
- An additional 31% reported losses between $10,000 and $200,000.
- 36% said they lost less than $5,000.

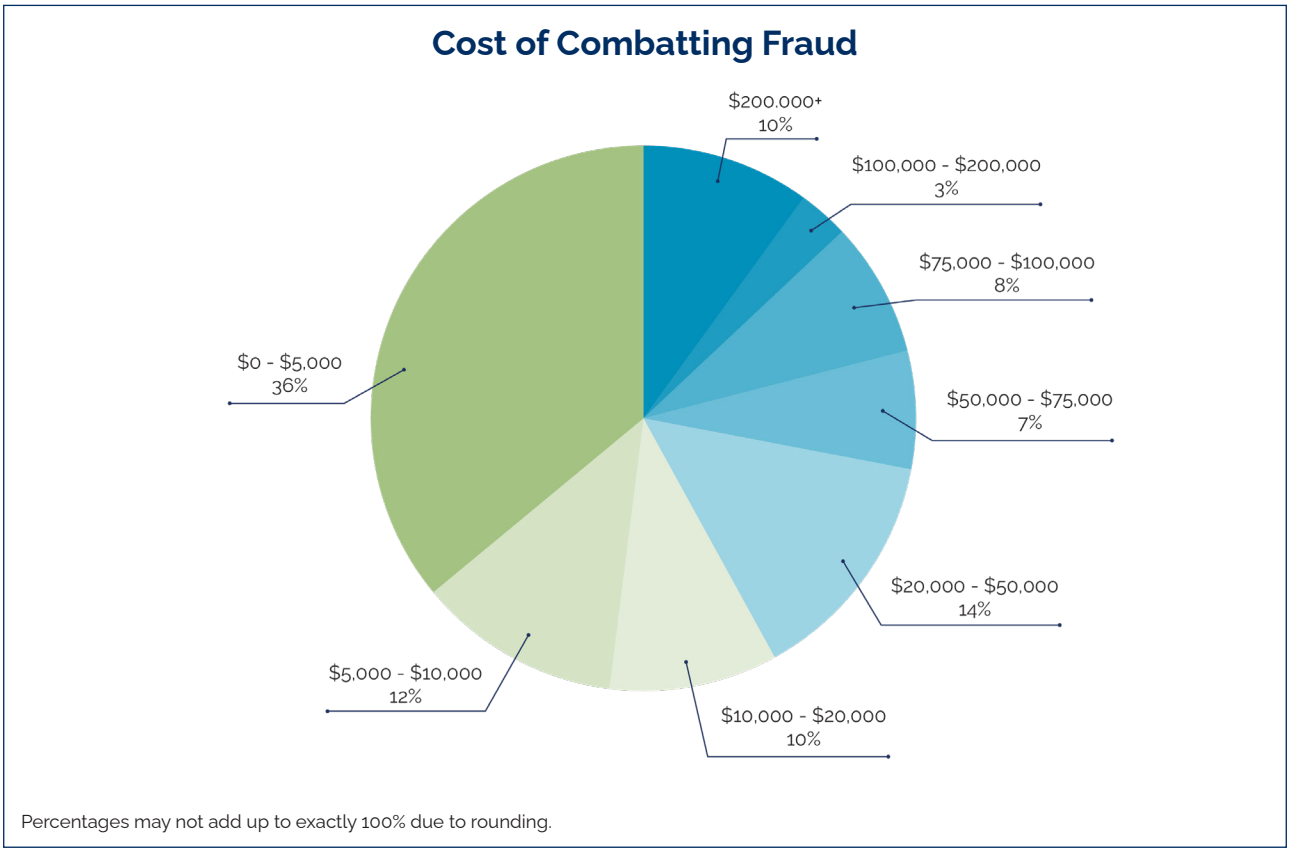
Estimated Financial Loss Due to Fraud



Percentages may not add up to exactly 100% due to rounding.

Fraud prevention isn't free either.

- 10% reported spending more than $200,000 in prevention-related costs.
- 51% of respondents spent between $5,000 and $100,000 on tools, staff time, insurance, and training.
- Again, 36% spent less than $5,000, similar to loss amounts reported.

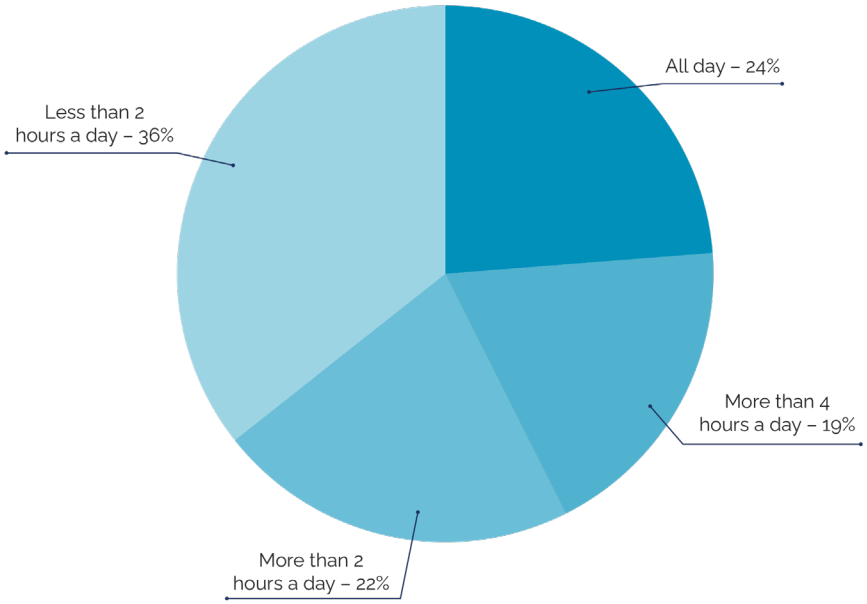


Time Spent on Fraud Prevention

The time commitment remains a key issue:

- 65% of respondents said they spend more than 2 hours per day, on average, preventing fraud each quarter—including 24% who spend the entire day.
- Only 36% spend less than 2 hours a day on prevention.

Time Spent Preventing Fraud Each Quarter

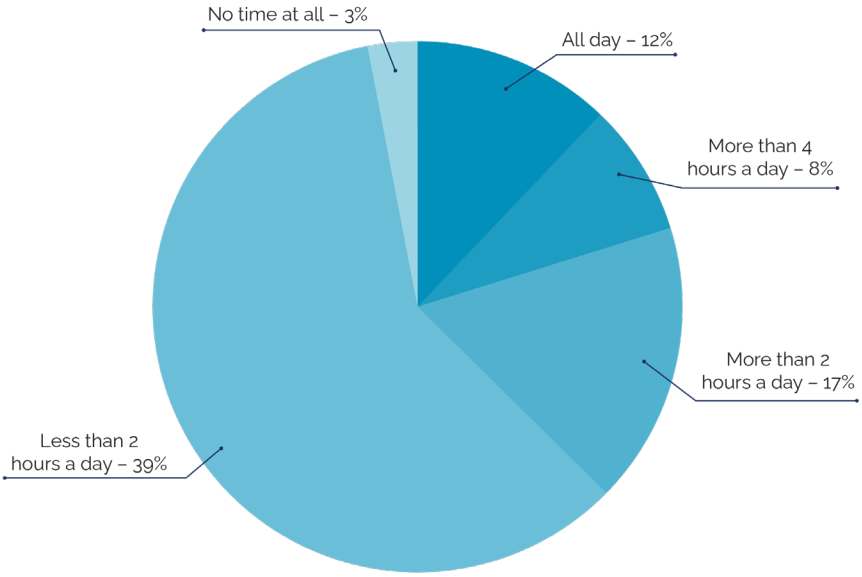


Percentages may not add up to exactly 100% due to rounding.

When dealing with fraud that does occur:

- 37% said their employees spend more than 2 hours a day responding to attempted or successful fraud, and 12% spend an entire day.
- 59% spend less than 2 hours.

Time Spent Preventing Fraud Incidents Each Quarter



Percentages may not add up to exactly 100% due to rounding.

Fraud Prevention Efforts

Consistent with our last report, **94% of survey respondents** detailed the measures they have in place to combat fraud—underscoring continued, significant investments in prevention across the industry. These efforts range from advanced technology adoption to process improvements and staff training. While companies vary in the tools they deploy, the overall picture is clear: prevention is no longer optional—it's a necessary cost of doing business.

The most commonly cited fraud mitigation and vetting strategies include:

- Verifying carrier authority, insurance, and safety records through multiple trusted sources
- Monitoring for recent contact or ownership changes
- Confirming emails and phone numbers against established records
- Avoiding first-time or unknown carriers on high-value or high-risk loads
- Using internal "Do Not Use" lists and flagging suspicious activity
- Conducting real-time load tracking and equipment verification
- Requiring supporting documentation such as proof of delivery, VINs, or photos
- Implementing standardized internal protocols and employee training programs
- Collaborating with peers and industry networks to share intelligence and red flags

ERIC ARLING | IEL FREIGHT | CINCINNATI, OH

Eric Arling at IEL Freight shared an alarming case of cargo theft that underscores the growing sophistication of this criminal enterprise. His company experienced two separate copper thefts from a client who primarily ships aluminum, with copper making up only 10% of their total shipments. Yet, both stolen loads were copper—a striking coincidence that suggests thieves were strategically targeting high-value freight.

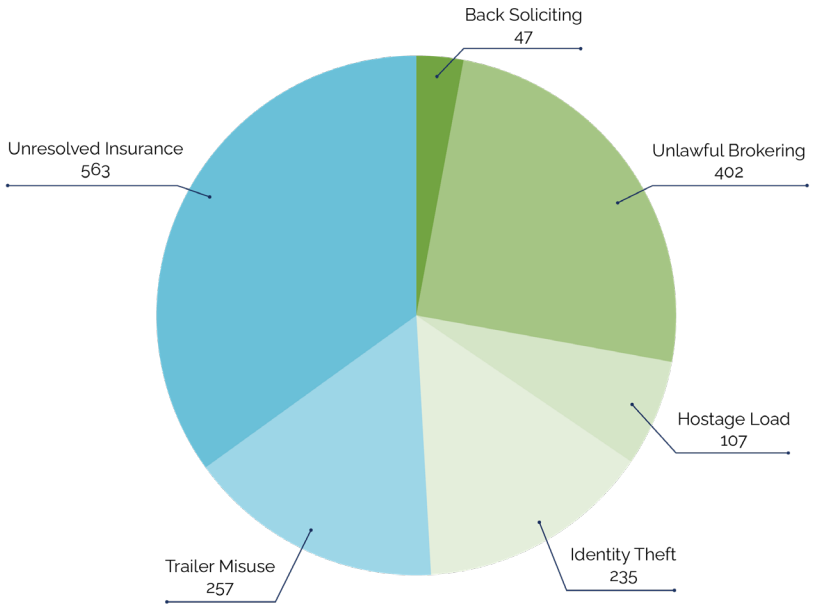
Through an internal investigation and collaboration with the shipper, Eric's team uncovered that criminals were using industry knowledge to identify and intercept specific shipments. Since only a handful of smelting facilities in the U.S. process copper in this form, thieves were able to infer the cargo type simply by recognizing the destination.

"The fact that both stolen shipments were copper, despite aluminum making up 90% of our client's shipments, made it clear that this wasn't luck—these criminals knew exactly what they were doing," Eric explained. "This wasn't just a random theft; it was a well-planned operation that exploited gaps in supply chain security."

What made this case stand out even more was the shipper's response. Rather than treating the thefts as isolated incidents, they worked closely with Eric's team to develop stronger vetting processes, and a new set of security protocols tailored specifically to high-risk shipments. "For the first time, we saw shippers not just expecting a solution from us but actually sitting down to collaborate on preventing future thefts," Eric said.

TIA Watchdog, a core resource for fraud reporting, has seen a substantial uptick in activity. From **September 1, 2024 through February 28, 2025**, there were **1,611 fraud reports** filed across seven key categories—an increase of **65%** compared to the prior eight-month reporting period included in our previous report. This dramatic rise underscores the continued escalation of fraudulent activity within the 3PL industry.

TIA Watchdog Reports | Sept 1, 2024 – Feb 28, 2025



Percentages may not add up to exactly 100% due to rounding.

Watchdog allows members to act quickly—flagging suspicious actors, checking active reports before engaging with new carriers, and sharing critical intelligence across the TIA network. As fraudulent tactics become more strategic and coordinated, this kind of peer-to-peer transparency is more vital than ever.

Despite these proactive efforts, fraudsters continue to adapt. The evolving nature of scams—including email spoofing, cargo diversions, and falsified identity documents—demands continuous vigilance and an ever-evolving fraud prevention strategy.

WHAT STEPS DOES YOUR COMPANY TAKE TO VET CARRIERS AND MITIGATE FRAUD RISK?

"Thorough vetting via multiple platforms. Real time compliance monitoring. Newly onboarded carriers aren't allowed to haul high value or targeted commodities."

"We use a vetting service and have our own internal vetting procedures as well."

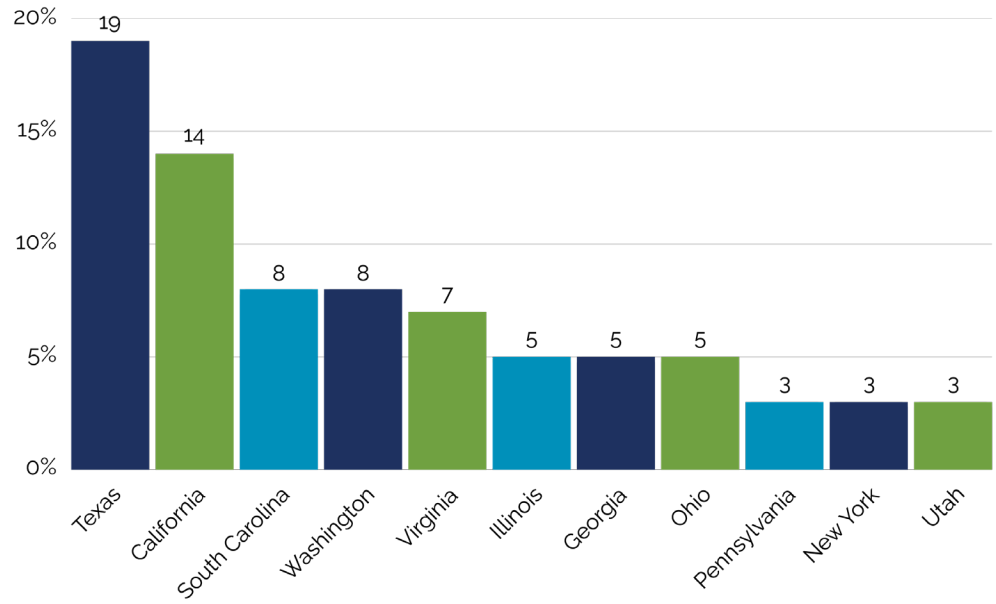
"Extensive background information checks on any new carrier in network, phone/address/email verifications routinely, cross referencing of tractor and trailer identification (VINs and plates). Use several outside vetting tools or software."

Geographic Distribution of Fraud

Fraud is heavily concentrated in a few states:

- 80% of reported fraud originated from just 11 states.
- Texas (19%) and California (14%) topped the list, followed by South Carolina and Washington (8% each).

Top States Where Fraud Originated

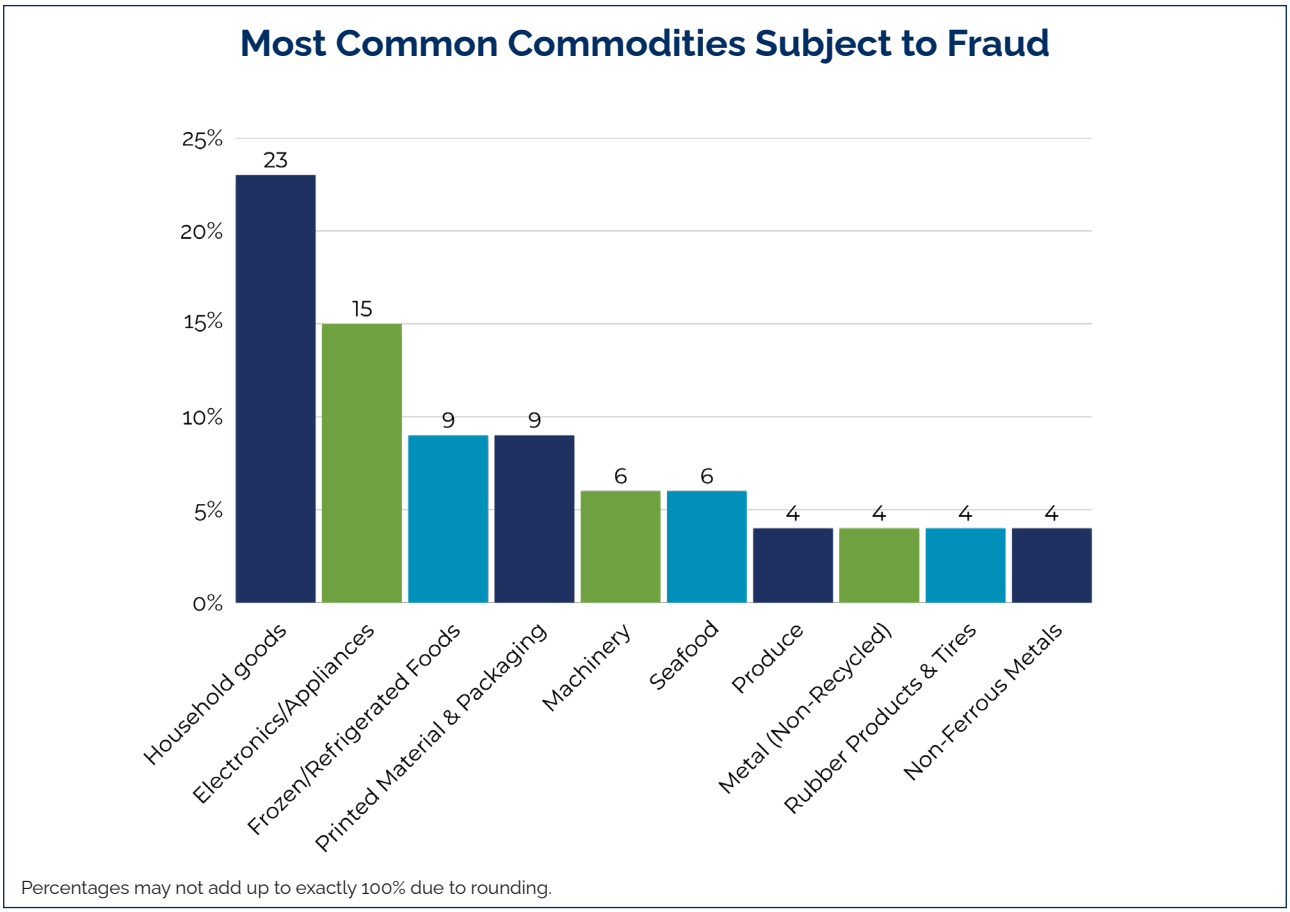


Percentages may not add up to exactly 100% due to rounding.

Commodities Most Affected

Certain commodities continue to be targeted for their resale value and accessibility. The most at-risk categories included:

- Household Goods (23%)
- Electronics/Appliances (15%)
- Frozen/Refrigerated Foods (9%)
- Printed Material & Packaging (9%)



Businesses moving these high-risk goods should consider implementing additional security protocols to reduce vulnerability.

Strategic Recommendations

Best Practices for Fraud Prevention

To effectively combat freight fraud, companies must adopt a multi-layered and proactive approach. This includes rigorous carrier vetting procedures, strong internal protocols, continuous employee training, and swift implementation of updated risk mitigation practices. In addition to onboarding standards and verification steps, companies should have internal escalation processes when red flags appear.

TIA's new Post-Fraud Incident Checklist was developed to support this effort, offering clear steps companies can take in the immediate aftermath of a fraud event. From internal reporting to legal follow-up, the checklist helps members minimize damage and prevent repeat incidents.

Collaborative Industry Action

Fraud is not a problem any one company can solve alone. It requires a united front from brokers, shippers, carriers, factoring companies, insurers, and vendors. TIA continues to bring the industry together by facilitating dialogue and encouraging shared standards across the ecosystem. Member platforms like Watchdog and peer forums have become vital for real-time alerts and pattern detection.

Regulatory Accountability

Fraud is no longer a nuisance—it's a national economic and security threat. As criminal tactics become more strategic and more global, law enforcement and federal regulators must act with urgency.

TIA urges FMCSA and Congress to focus on policies that truly strengthen the supply chain. Specifically:

- Remove illegitimate carriers and brokers from FMCSA databases.
- Crack down on cargo theft and strategic fraud—a problem costing the industry tens of billions annually.
- Support legislation such as the Safeguard Our Supply Chain Act to establish a federal task force on cargo theft.

The continued inaction and jurisdictional confusion leave small businesses and large enterprises alike with little recourse. That must change.

Invest in Scalable Technology

As fraud evolves, technology must too. Members report investing in tools for identity verification, real-time monitoring, and secure communications. However, the burden is disproportionately placed on brokers. The industry needs scalable, vendor-neutral solutions and shared intelligence to keep pace with fraud's accelerating sophistication.

The Path Forward: Building a Resilient Industry

Long-Term Impact

Fraud is more than a line-item loss. It destabilizes relationships, weakens trust across the supply chain, and ultimately drives up costs for shippers, businesses, and consumers. For small and mid-size 3PLs, a single major incident can have devastating consequences. Preventing fraud is not just a matter of business operations—it's a strategic imperative.

TIA's Commitment

TIA will continue to support its members through:

- **Policy advocacy** for regulatory reform and enforcement.
- **Education and resources** such as the Fraud Report, Watchdog platform, and Post-Fraud Incident Checklist.
- **Conversations and coalitions** that unite stakeholders across the supply chain to fight fraud collectively.

TIA is also exploring the possibility of a future industry-wide summit to address this issue head-on and develop cross-sector solutions.

Call to Action

The industry must remain vigilant—and vocal. Now is the time to:

- Review and strengthen your fraud prevention protocols.
- Engage with TIA tools and peer communities to share insights and alerts.

- Urge regulators and lawmakers to take decisive, coordinated action against the growing fraud epidemic.

Fraud may be evolving—but so is our collective response. Together, we can build a more secure and resilient supply chain.

Methodology

Survey Data Collection

The data presented in this report was collected through an online survey conducted by TIA from January 2, 2025 through February 6, 2025. The survey was shared with TIA members who are professionals working at third-party logistics companies, and 59 responses were submitted. Respondents were asked to share their experiences with various types of fraud, the financial impact of these incidents, and the measures they have implemented to prevent and respond to fraud. The data was then analyzed to identify key trends, fraud patterns, prevention efforts, and resource burdens.

In addition to survey responses, this report incorporates incident data from TIA Watchdog covering the period from September 1, 2024, through February 28, 2025. Watchdog is a reporting tool that allows brokers to share fraud incidents in real time to help protect the broader community.

Together, these two data sets provide a grounded, real-world snapshot of how fraud continues to evolve and how logistics companies are responding.

Limitations

While the survey provides valuable insights into the state of fraud within the logistics and transportation industry, there are certain limitations to consider. The survey sample, while representative of TIA's membership, may not fully capture the experiences of all industry participants. While the sample size represents a small portion of TIA's full membership, the responses provide valuable directional insights into how fraud is impacting 3PL companies across the industry. Additionally, the self-reported nature of the data may introduce some bias, as respondents may not always accurately recall or report incidents. Despite these limitations, the findings offer a robust overview of the challenges and opportunities in combating fraud within the industry.

Future Outlook

Freight fraud is not subsiding—it is evolving. New tactics, more complex schemes, and increased financial losses are shaping a new normal. As criminals become more coordinated, so must the industry.

TIA will continue to lead the fight by producing regular fraud reporting, advancing member tools like Watchdog, pushing for federal action, and empowering logistics companies with actionable resources like the new Post-Fraud Incident Checklist.

Moving forward, protecting the supply chain will require constant vigilance, smarter regulation, industry-wide collaboration, and scalable tools that adapt as fast as the criminals do. TIA is committed to helping members navigate these challenges and strengthening the collective response to freight fraud across the country.