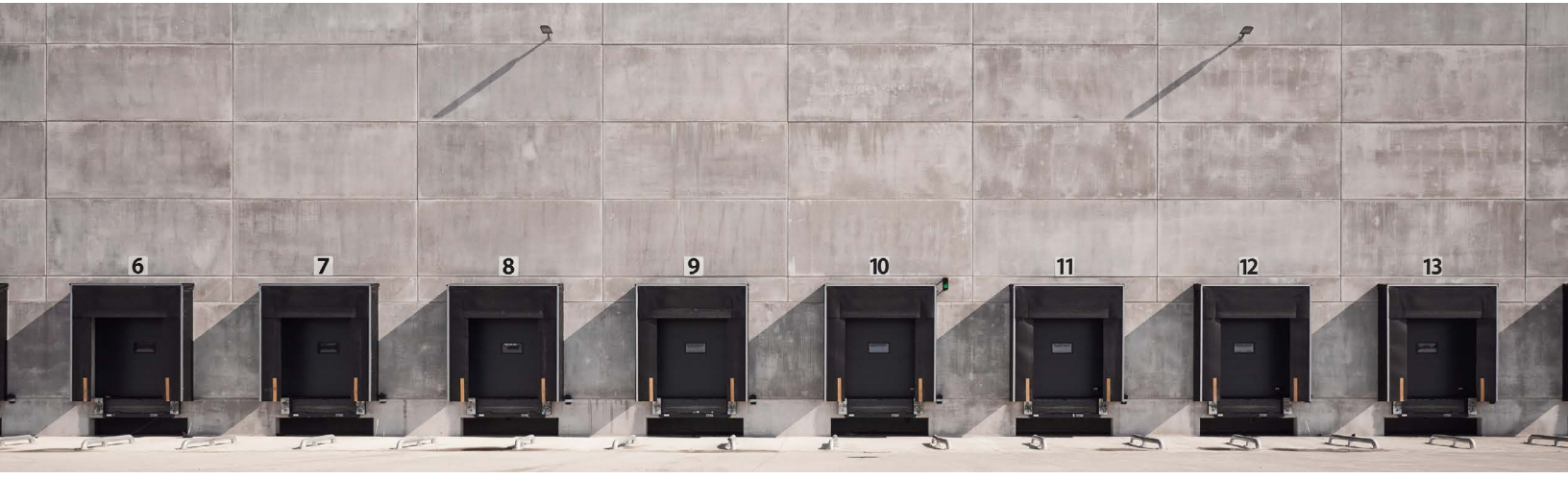
Uber Freight

Navigating freight fraud

A guide to safeguard your supply chain

Table of contents: What's in our guide



No business sector is safe from transportation theft. Whether you're moving consumer electronics or food and beverage products, your company could be at risk of fraudsters stealing your goods. In fact, criminal activity within the freight industry is on the rise: estimates say that reports of fraud jumped 400% in 2022 and steadily increased throughout 2023.

If left uncontrolled, transportation fraud can cause major supply chain delays, miscommunication, and customer dissatisfaction. While the crime will never subside completely, you can take proactive steps to identify and handle bad actors in your network. At Uber Freight, our team of experienced fraud investigators stays on the pulse of the evolving fraud landscape. They work tirelessly to help shippers protect themselves against schemes like pilferage and identity cloning.

From using technology to identify user behavior anomalies to investing in fraud education, you have an opportunity to take action and safeguard your supply chain for the future.

The impact of fraud on your bottom line

$1 billion: the amount the freight industry loses to fraud each year, according to the Transportation Intermediaries Association (TIA) estimates.

Thieves stole more than **$31.1 million** in shipments in Q3 of 2023, according to CargoNet.

Cargo theft is a **$15 to $35 billion industry**, reports the National Insurance Crime Bureau.

Cargo fraud 101: Understanding common schemes

As the industry shifts to more automated, tech-enabled transportation management, bad actors have become more savvy in committing fraud and theft online.

> Rapid digitization of logistics operations has led to a more calculated, organized approach to fraud.
>
> — Bill McDermott, Uber Freight Senior Investigator

Three prominent types of fraud in today's industry are online identity theft, pilferage, and double-brokering.

1. Identify theft

Criminal groups often use online platforms to interact with logistics teams by posing as credible carriers or brokers. These acts are commonly known as phishing or digital identity cloning—and transportation is the ninth most targeted industry for cyberattacks.

Fraudsters build fake websites, use fake email addresses, or even manipulate electronic records like destination details and delivery schedules. They can also submit fake orders that lead to misdirected shipments and unauthorized stops, allowing them to target their intended cargo for monetary gain.

In one instance, an account manager reported to Uber Freight that they'd received suspicious emails asking about a specific load posted to a load board. The perpetrator had created fake company names, logos, and web addresses designed to be familiar enough to trick an operator into tendering a shipment. Thankfully, the account manager used what they learned from internal training to catch these anomalies, and did not tender the load to the fake carrier.

2. Pilferage

Pilferage scams, in which thieves steal small quantities of goods rather than entire truckloads, are common and hard to detect. Your distribution center could receive the exact number of pallets it was supposed to receive in a shipment, but surprise: when you open the pallets, each one is missing a small amount of units.

Bad actors often opt for pilferage scams because it reduces the chance they have of being caught, as it takes longer for shippers to discover theft has been committed. They can use sneaky tactics, such as tampering with truck seals and altering bills of lading, to get away with the crime.

3. Double-brokering

The fraud scheme involves people accepting loads from brokers, then posting them on public load boards where they assign the loads to carriers. People can double their profits from tendering a single shipment, while carriers in on the scheme can steal the goods and also receive double payments. Double-brokering is responsible for $500 to $700 million in lost payments annually.

Effectively tackling these fraudulent activities requires a multifaceted approach of using the logistics technology and data at our disposal, collaborating with third parties to expand information sharing, and relying on human expertise to spread the knowledge across business organizations internally.

Don't forget to vet your carriers

One of the best ways to safeguard against fraudulent behavior is to vet your carriers. To further reduce risk, be sure to consider the following when vetting your carriers:

- Verify their USDOT and MC numbers, and insurance information.
- Check their compliance with operating authority and FMCSA safety ratings.
- Confirm they're reliable by assessing OTIF performance and checking with other companies they've worked with in the past.
- Scan TIA Watchdog reports to see if there's a history of issues.

Use logistics technology to identify anomalies

Pinpointing suspicious activity within starts with 360° visibility into a company's logistics network. Today's tech-driven transportation management system (TMS) can continuously analyze order processing, carrier profiles and their historical behaviors, shipment tracking, and financial transactions. It can also monitor login times and access permissions to uncover anything that might suggest suspicious activity.

The more information you have, the better chance you have to catch bad actors.

The end objective is to use the shipping information at your disposal to set KPIs that define what qualifies as a deviation from the norm—making it easier to identify, flag and investigate suspicious activity.

> Information is key. That means leveraging any and all internal and external data sources available to create a robust overview of user identity and behavior. It helps tell a story that can better identify emerging bad actors.
>
> — Alexis Watkins, Senior Manager, Carrier Risk and Compliance at Uber Freight

Know the signs of freight fraud

Examples of anomalies that could indicate scams include:

- Freight documentation inconsistencies
- Unverifiable broker or carrier company details
- Unexpected detours in transit
- Altered methods of payment
- Sudden communication drops with carriers

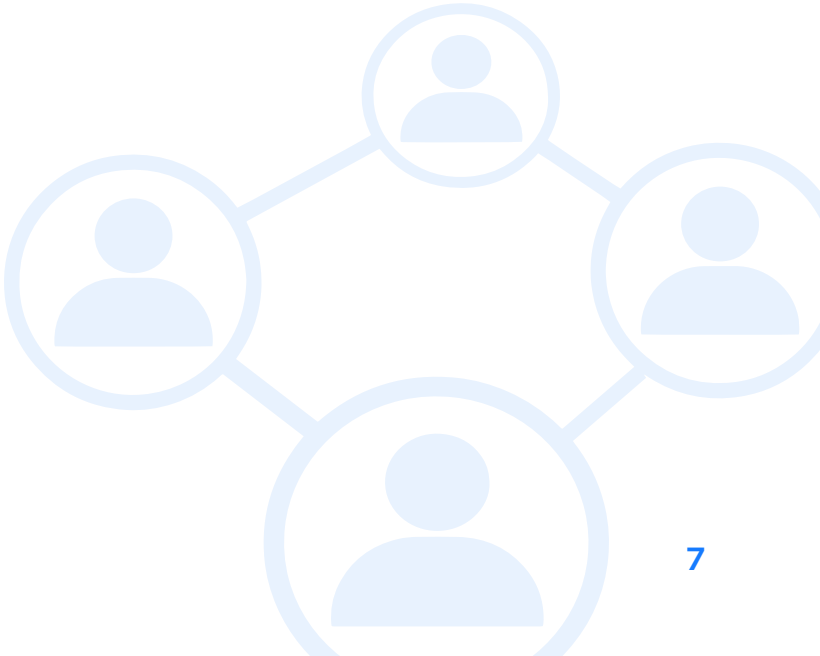
Collaborate with third parties to combat criminals

While access to real-time tracking data will undoubtedly help you stay on top of potential criminal activity, technology alone isn't enough. Working with fraud experts and industry counterparts—will be critical to the fight against cargo theft.

The supply chain is a collaborative business, with multiple parties involved at each stage. And it's undoubtedly competitive from a pricing perspective, but the competition to save on costs is exactly what fraudsters are exploiting. If we don't work together, the entire industry will suffer.

Criminals tend to target multiple factions within a network, so be sure to establish and keep an open channel of communication with other industry stakeholders, including fellow shippers, and use that channel to share findings. Reporting suspicious activity to organizations dedicated to fighting fraud, such as CargoNet and TIA Watchdog, will also help spread useful information across the industry.

> “
>
> Sharing information doesn't take away your competitive edge. No one—and I mean no one—can succeed if fraud continues to run rampant.”
>
> — Bill McDermott, Uber Freight Senior Investigator



Invest in fraud prevention training

Fighting fraud is a complex challenge that can occur at any stage of the supply chain. It's vital that everyone across your organization, from sales personnel to logistics operators, is armed with the knowledge needed to spot it. Cases can often manifest first by targeting specific frontline workers who may not know how to spot a bad actor.

Invest in training programs and conduct hands-on exercises to ensure everyone across your company becomes more experienced in identifying suspicious activity. Beyond formal education, encourage open lines of communication for employees to report concerns, share useful insights, and ask questions.

Logistics is a fast-paced industry by nature, but a company culture where everyone feels empowered to fight fraud will ultimately make it easier to safeguard the supply chain moving forward.

Ready to build a more secure supply chain?
Connect with an Uber Freight representative today.