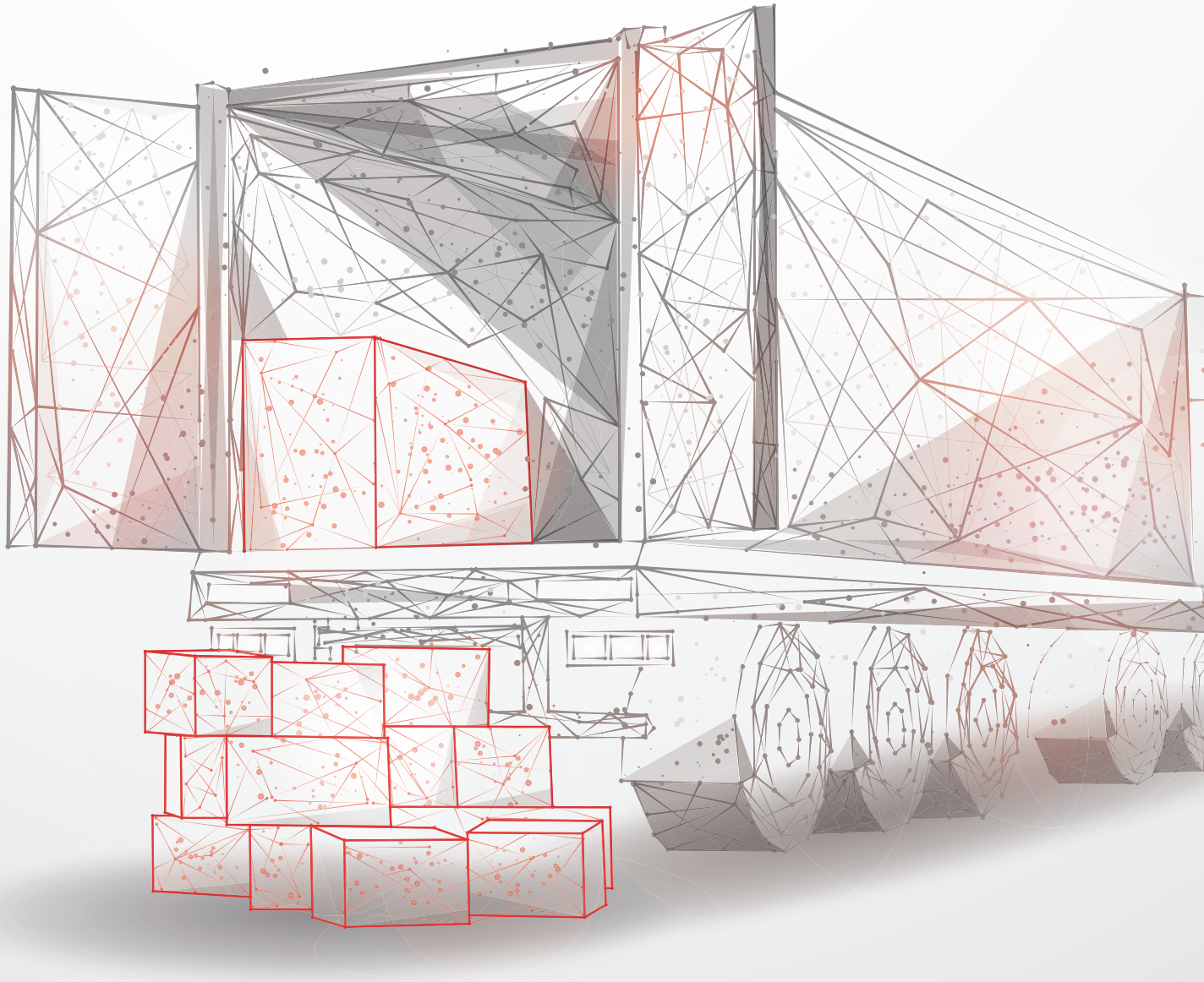
SPOT



FROM BLIND SPOTS TO BEST PRACTICES

Combating Cargo Theft in Today's Freight Market

Contents

Cargo theft is a growing concern across the supply chain, affecting shippers, carriers, and logistics providers alike. As criminal tactics become increasingly sophisticated, it's more important than ever for organizations to stay informed and prepared.

We've written this guide to help you better understand current cargo theft trends, the common tactics used by bad actors, and the proactive steps shippers can take to reduce risk and respond effectively when theft occurs.

In the sections that follow, we'll cover:

- Current market trends in cargo theft
- How common theft tactics are executed
- Practical guidelines for prevention at the shipper level
- What to do when a cargo loss occurs

Whether you're looking to strengthen internal protocols or better align with transportation partners in a high-risk environment, this guide gives you the clarity and tools needed to act confidently.

Cargo Theft Trends: A Growing Threat to the Supply Chain

In 2024, reported thefts increased by 27 percent compared to 2023, rising from 2,854 incidents to 3,625[1]. The trend has continued into 2025, with second-quarter data revealing 884 reported thefts[5]. This marks a 13 percent increase compared to the same period in 2024 and a 10 percent rise from the first quarter of 2025[3].

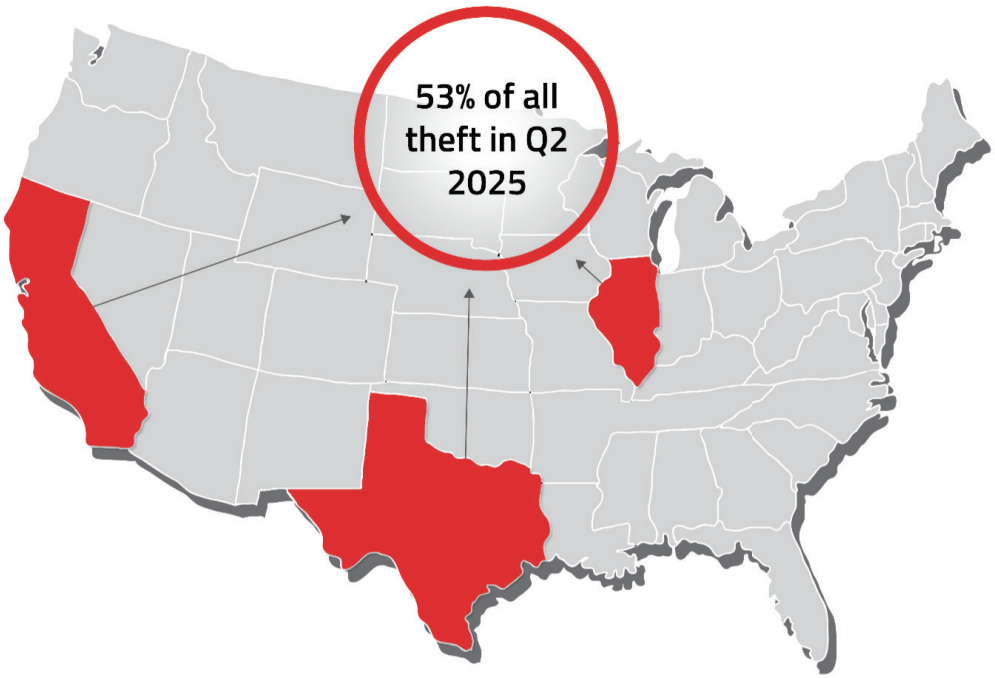
The financial impact is also significant. When applying average loss values to incidents that did not include specific amounts, **the total estimated loss for Q2 2025 exceeds 61 million dollars.**

Data from April through June 2025 shows that theft activity is accelerating. April saw a 14.6 percent increase in incidents, followed by a 4.4 percent rise in May. In June, thefts surged by 21.9 percent, signaling a sharp escalation in criminal activity[5].

Hotspots for Cargo Theft Activity

Cargo theft risk varies significantly by region and is closely tied to freight volume, urban warehousing trends, and weak points in infrastructure. These factors often intersect with the operations of organized criminal networks, creating persistent hotspots for theft.

According to CargoNet's 2025 Second Quarter Risk Trends Analysis, cargo crime remains heavily concentrated in a small number of states. In Q2 2025, Illinois emerged as one of the top three states for theft, replacing Florida. Together, the top three states now account for 53 percent of all reported thefts during the quarter. This represents a relative increase of 17.78 percent compared to the previous quarter[5].

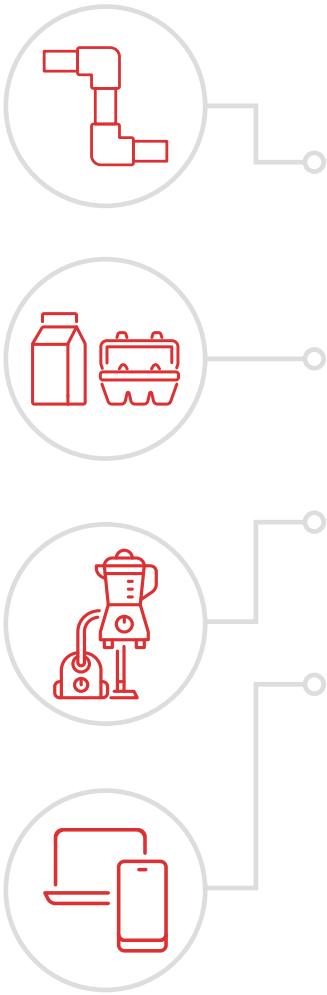


Where Freight Theft Happens Most

The majority of cargo thefts take place at shipper-controlled facilities, with **warehouses and distribution centers** consistently ranking as the most frequently targeted pickup locations. These sites often suffer from preventable security weaknesses, including insufficient perimeter fencing, minimal surveillance during nights and weekends, and limited verification procedures for drivers and carriers. These gaps are routinely exploited by organized theft rings that coordinate their actions to remove freight quickly and without resistance. Additionally, in many cases, these locations are vulnerable due to insider risk, where employees or contractors exploit their access and knowledge of weak points to facilitate theft. They are also the front lines for fraudulent tactics further described herein.

Truck stops represent the second most common setting for cargo theft. Like warehouses, they are vulnerable due to a lack of real-time monitoring and a breakdown in chain-of-custody protocols. The absence of strict oversight at these sites allows criminals to act without immediate detection[5].

High-Value Targets: Commodities Most at Risk in Cargo Theft



In terms of what is being stolen, organized theft groups continue to prioritize certain types of commodities based on market demand, ease of resale, and the challenge of traceability.

Metal shipments, especially copper, have seen the most dramatic increase in theft. There were 53 reported incidents involving metals in Q2 2025, nearly double the previous year, representing a 96 percent year-over-year surge. This spike aligns with copper trading near record highs, suggesting that theft activity is influenced by commodity market fluctuations.

Food and beverage products have also become increasingly common targets. There were 180 reported thefts in Q2 2025 alone, marking a 68 percent increase compared to the same period in 2024. These items now represent more than 20 percent of all cargo theft, with alcohol, energy drinks, and meat among the most frequently stolen[5].

Household goods continue to be a major area of loss, including appliances, furniture, and other high-value home products. These bulky but lucrative items are often stolen during long-haul or final-mile transportation, particularly when left in unmonitored trailers or stored in facilities with inadequate oversight.

Electronics remain a constant target, with items such as televisions and computers drawing the attention of organized crime due to their strong aftermarket value. These products are typically intercepted during transfer points in the supply chain, where verification and monitoring are weakest[1].

In short, cargo thieves are not just opportunistic; they are strategic. They prioritize loads that combine value, volume, and low traceability, making these categories especially important for shippers to protect[1].

Average Loss Per Theft: $204K

How Freight Gets Stolen:
Tactics Behind the Threat

Cargo theft today isn't what most people imagine. It doesn't look like a truck hijacking or a cinematic chase; it's quieter, more calculated, and it often happens under the radar. Many of the incidents start with small gaps in everyday processes: a name that isn't double-checked, a trailer that looks mostly fine, a placard that looks questionable. But behind these moments are tactics deliberately designed to exploit trust, routine, and speed.

Impersonation and Identity-Based Deception

Showing Up as Someone They're Not (Carrier Impersonation)

One of the most common tactics is simple: a truck arrives, the driver checks in, and everything seems normal, until it's not. The truck might have a magnet or a printed placard taped on the door to look legitimate. The name matches the paperwork, but no one verifies what's actually on the vehicle. In reality, the driver doesn't work for the company listed, and once the freight is loaded, it disappears.

Tricking Both Sides (Fictitious Pickups)

This tactic is particularly deceptive. Fraudsters pretend to be a broker, book a load, then impersonate a carrier to hand it off to an unsuspecting legitimate driver. That driver thinks they're hauling a real load, but they've been told to deliver it to the wrong location. The freight is rerouted and offloaded before anyone realizes what's happened.

Losing the Trail (Double Brokering)

Sometimes the load delivers, but not by the carrier who was hired. In one version of this scheme, the real carrier never gets paid and starts calling the shipper or receiver, demanding answers. In the worst-case scenario, the load is passed off and vanishes entirely. Either way, the result is confusion, conflict, and risk.

Using Confusion to Cover Theft (Blind Shipment Abuse)

Blind shipments are a normal part of some logistics networks, but they're also a tactic for theft. Drivers may be told the destination is different than what's listed on the BOL. If no one asks questions, the load can be quietly delivered somewhere it was never supposed to go, and no one knows until it's too late.

Mid-Transit Manipulation and Concealed Theft

Breaking in Without Breaking the Seal (Seal-Intact Pilferage)

Even seals aren't always what they seem. Thieves have learned how to dismantle trailer doors from the outside, carefully removing bolts to open the back, remove part of the cargo, and reseal everything. On the surface, the load appears untouched, until someone looks closer and realizes entire pallets are missing. Thieves often pair this tactic with altered paperwork to cover their tracks (see below).

Changing the Story Mid-Route (Paperwork Modification)

Bills of lading (BOLs) are still largely handled on paper or PDF. Thieves know this, and take advantage of it. A load of 20 pallets leaves the shipper, but the paperwork is edited somewhere along the way to say 12. When the receiver signs off, no one realizes the loss until weeks later during inventory. By then, the trail is long cold.

Diverting the Load Mid-Trip (In-Transit Theft)

Sometimes the theft doesn't happen at pickup, it happens while the truck is already on the road. A driver might report a breakdown, or delay delivery while the freight is quietly offloaded at a cross-dock, broken into smaller shipments, and moved again. By the time someone notices something's wrong, the cargo is long gone.

Digital Intrusion and Credential Exploitation

Getting in Through the Inbox (Email Compromise)

Phishing emails are becoming a gateway to cargo theft. Posing as the DOT or other freight-related entity, thieves trick carriers into sharing login credentials. Once inside, criminals monitor inboxes, intercept load details, and manipulate communication from behind the scenes, sometimes for weeks, without raising alarms.

Another common tactic: impersonation through nearly identical email addresses. Thieves register domains that look legitimate at a glance, swapping a letter, adding a hyphen, or replacing "inc" with "Inc", and use those modified emails to pose as trusted carriers or brokers. They insert themselves into active load negotiations, tender freight under false pretenses, and arrange pickups that never reach their destinations. By the time anyone notices, the cargo, and the criminal, are long gone.

Buying a Carrier Identity (Fraudulent Authority Transfers)

When carriers go out of business or sell their MC number, bad actors are waiting. They scoop up legitimate authorities and use them to book freight under false pretenses. These scams often involve sudden changes to insurance policies, contact info, or ownership, moves that look innocent unless you're watching closely.

These tactics are growing more sophisticated, and they're targeting the weak spots in everyday workflows. It's not just about security systems or background checks; it's about paying closer attention to the small moments where things can go wrong[4].

The Four Stages of Cargo Theft Prevention

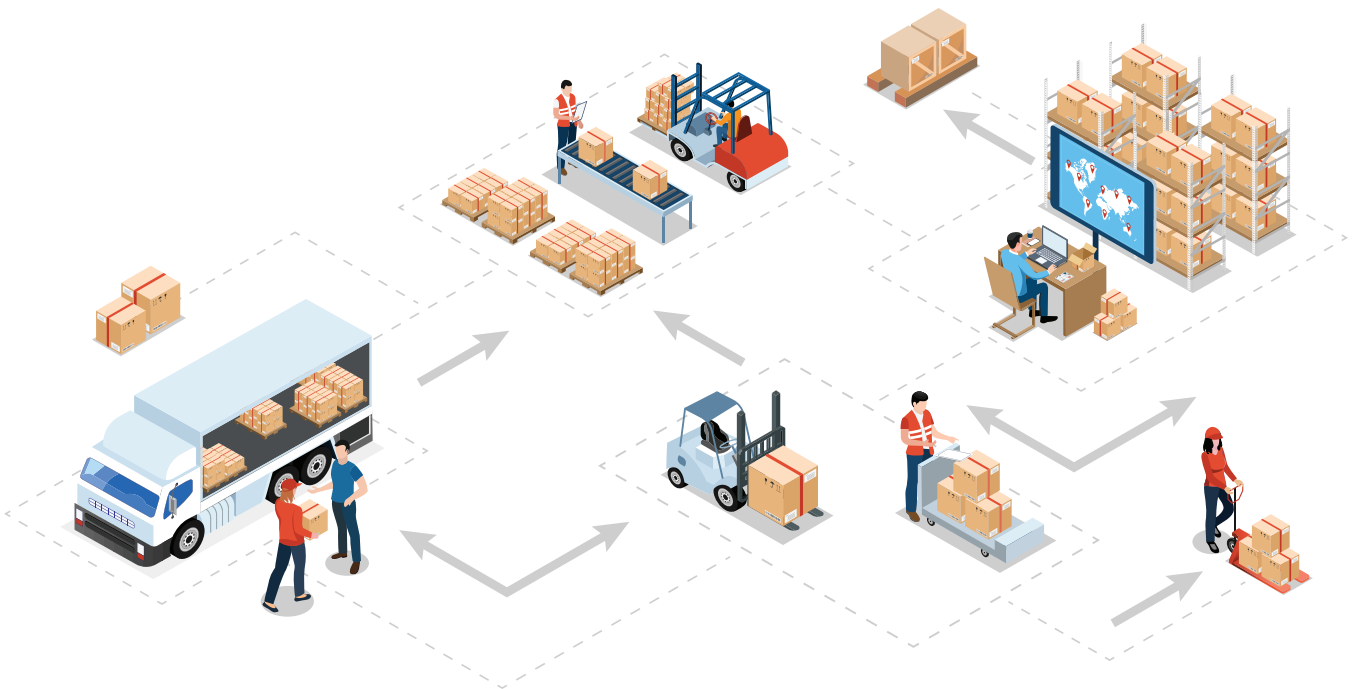
Cargo theft doesn't usually start with a ski mask and a getaway truck. It often begins with an unchecked email, a missed phone call, or a clipboard handed to the wrong driver. It's subtle. It's strategic. And it's becoming more sophisticated every day.

That's why prevention needs to start well before the truck arrives and continue all the way through delivery. It requires a proactive mindset and clear communication across every step of the shipment process.

The four stages below outline what to watch for, who to verify, and how to spot red flags before they turn into costly problems.

1. Carrier Validation (Before Pickup)

- **Vet carrier legitimacy:** Ensure the carrier's authority hasn't changed hands recently and their insurance, safety record, and contact information are up to date.
- **Monitor red flags:**
  - » Recent changes in phone/email.
  - » Changes in ownership or authority status.
  - » Unusual insurance activity.
- **Email security concerns:** Require brokers and carriers to use secure portals or multi-factor authentication instead of unencrypted emails, which can be easily compromised.
- **Broker accountability:** Understand how your broker screens carriers, how they transmit load info, and if they use secure channels (not just email).



2. At Pickup (Shipper-Side Verification)

- **Match driver and vehicle info:**
  - » Physically inspect trucks for fake placards or paper logos.
  - » Confirm DOT numbers and driver name with the expected carrier.
  - » Make photocopy of driver's CDL.
- **Validate contact details:**
  - » Call the phone number the driver provides on the spot to verify identity.
  - » Ask drivers if they were instructed to check in under another company name.
- **Control documentation:**
  - » Do not pre-print BOLs with the broker's name listed as carrier.
  - » Write the actual motor carrier name and contact info on all paperwork.
- **Photo documentation:**
  - » Take pictures of the freight inside the trailer.
  - » Photograph trailer seals, trailer number, license plates, and tractor sides / door panel.
  - » Store photos in a shared load confirmation packet with brokers/receivers.
- **Confirm destination and awareness:**
  - » Ask drivers where they are delivering the load and confirm it matches the BOL.
  - » Educate drivers on fictitious pickup scams and their potential liability.

3. In-Transit Monitoring

- **Use multiple tracking methods:**
  - » GPS trackers inside trailers.
  - » Driver phone apps.
  - » ELD (Electronic Logging Device) tracking.
- **Use trailer sensors:**
  - » Light, shock, and door sensors can alert when tampering is detected.
- **Cross-check data:** Discrepancies between driver and trailer location can reveal theft in progress.

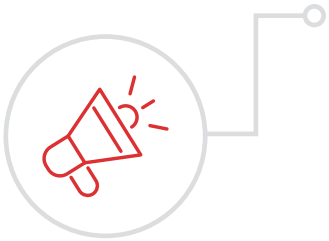
4. The Role of Communication

- **Open shipper-broker communication:**
  - » Know exactly who is picking up the load. If an asset-based carrier is approved to be transporting a load, ensure the load is not brokered to a different carrier.
  - » Share all load, truck, and driver info ahead of time.
  - » Ensure broker 24/7 contact information is provided.
- **Empower onsite staff:**
  - » Train guard shacks and dock staff to verify paperwork, photos, and identities.
  - » Give them SOPs to escalate mismatched or suspicious drivers.

Post-Theft Response: **What to Do** When the Worst Happens

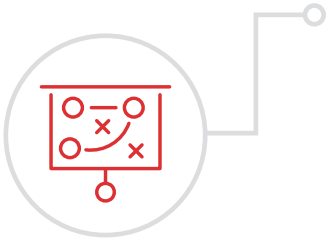
Even the most prepared shipper can fall victim to cargo theft. Once a load disappears, every minute matters. Delayed action gives thieves more time to vanish and lowers the odds of recovery. That's why a clearly defined, rehearsed response plan is just as critical as prevention.

Think of it like a fire drill. You hope you never need it, but if the alarm sounds, hesitation is not an option. Your ability to act fast, communicate clearly, and preserve key records can mean the difference between a total loss and a recovered load.



Step 1: Alert and Report Immediately

- **Contact law enforcement:** File a police report with the jurisdiction where the theft occurred, usually the pickup location or last known trailer position.
- **Notify CargoNet:** Submit an incident report through CargoNet's portal. Even non-members can report thefts, and doing so increases visibility among recovery networks.
- **Involve your insurer:** Reach out to your cargo insurance provider to initiate a claims/loss prevention and follow any specific documentation procedures they require.



Step 2: Activate Your Internal Response Plan

- **Designate a point person:** Assign a single coordinator, ideally on-site, to manage law enforcement interaction and coordinate updates across departments.
- **Notify key stakeholders:** Immediately inform internal teams such as logistics, claims, risk management, legal, and leadership so everyone is aligned.
- **Preserve documentation:** Secure and organize all load records, including bills of lading, photos, driver ID copies, carrier communications, tracking data, and any video footage if available.

Step 3: Leverage Tracking and Communication Tools

- **Access telematics:** Pull GPS logs, trailer sensor data, or electronic logging device information to pinpoint the last known location and any irregular movement.
- **Check communication logs:** Review recent emails and texts with the driver, broker, or carrier for inconsistencies, last contact, or suspicious changes.
- **Identify impersonation:** Re-examine the pickup process. Was the correct carrier confirmed? Were there placards, email domains, or phone numbers that seemed off in hindsight?

Step 4: Coordinate Recovery Efforts

- **Assist law enforcement:** Provide a full timeline of events, key documents, and contact information for the broker, carrier, and driver. If GPS is still active, share it immediately.
- **Work with CargoNet and insurers:** Stay in close communication and monitor alerts. Recovery often depends on fast collaboration across networks.
- **Flag bad actors:** If the theft involved impersonation or false paperwork, alert your broker network and industry peers to help prevent further losses.

Step 5: Conduct a Post-Incident Review

- **Hold an internal debrief:** Identify what went wrong, such as gaps in driver validation, email security, or physical site protocols.
- **Update your prevention plan:** Adjust your processes, retrain staff if needed, and document the incident in a central loss history log.
- **Use what you learn:** Share insights with your transportation partners. The more visibility you create around how thefts happen, the harder it becomes for thieves to succeed.

Final Thoughts

Cargo theft is a complex problem that is not going away any time soon. To combat this challenge, it will take shippers, brokers, carriers, and receivers working in lockstep to detect, prevent, and respond to this growing threat. We're committed to being part of that solution.

If you'd like to explore any of the topics covered here in more depth or understand how Spot protects your freight through layered security and validation protocols, don't hesitate to contact us.

Together, we can make cargo theft harder to execute and easier to prevent.

References

[1] CargoNet. (2024). CargoNet's 2024 Supply Chain Risk Trends. Verisk Analytics, Inc.

[2] CargoNet. (2025, January 1). 2024 Supply Chain Risk Trends Analysis. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-theft-trends/

[3] CargoNet. (2025). 2025 First Quarter Supply Chain Risk Trends Analysis. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2025-q1-theft-trends2/

[4] Krop, A., & Hunter, K. (2025, June). Cargo Theft Awareness. Spot.

[5] CargoNet. (2025). 2025 Second Quarter Supply Chain Risk Trends Analysis. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2025-q2-theft-trends/

Andrew Krop
Chief Financial Officer, Spot

317.854.6110

akrop@spotinc.com

spotinc.com