CTPAT Alert – Surge in Cargo Theft and Security Best Practices

Last Updated: March 17, 2026

Background

Cargo theft in the United States has surged dramatically across all transport modes—maritime, truck, rail, and air. Organized crime groups and sophisticated fraud schemes are increasingly targeting supply chains, resulting in significant financial losses and operational disruptions. According to recent industry reports, cargo theft costs the U.S. freight transportation industry $18 million each day, with 74% of stolen goods never recovered. Estimated losses surged 60% to nearly $725 million in 2025, and average theft value rose 36% to $273,990 per incident. Major increases have been observed in states such as New Jersey (+50%), Indiana (+30%), and Pennsylvania (+24%). High-value targets include food and beverage, metals (especially copper), enterprise computing hardware, and cryptocurrency mining equipment.

Cargo Theft Trends

- Shift from traditional theft by small crews to sophisticated, strategic theft by organized crime rings using deception, cybercrime, and fraud (e.g., fictitious pickups, double-brokerage scams, identity theft).
- Cybercrime is increasingly used to steal load board credentials and book legitimate loads before theft occurs, often undetected until tracking devices reveal the crime.
- Geographic dispersion of theft activity, with increased incidents outside traditional hot spots near ports and rail yards.
- High-value and selective targeting by organized groups.

Security Procedures and Best Practices

1. Written Procedures and Incident Reporting

- CTPAT Members must have written procedures for reporting incidents, including internal escalation and notification protocols for suspicious activities or security incidents (e.g., drug seizures, discovery of stowaways, container tampering, unauthorized entry, extortion, or use of business entity identifiers).
- Notifications to CBP and law enforcement must be made as soon as feasibly possible and in advance of any conveyance crossing the border. Procedures must include accurate contact information and be periodically reviewed.

2. Anonymous Reporting Mechanisms

- Members should establish mechanisms (e.g., hotlines) for anonymous reporting of security-related issues. All allegations should be investigated, corrective actions taken, and evidence retained to document investigations.

3. Internal Investigation Protocols

- Members must initiate internal investigations of any security-related incidents immediately after becoming aware, ensuring company investigations do not impede law enforcement.

4. Seal Security

- Maintain detailed, written high-security seal procedures, including issuance, control, and steps for handling altered or tampered seals. Investigate discrepancies and report compromised seals to CBP and relevant authorities.
- All shipments that can be sealed must be secured immediately after loading with ISO 17712-compliant high-security seals. Seal numbers should be transmitted to consignees and printed on shipping documents.
- When appropriate, high security barrier bar seals should be considered when transporting high value shipments.

5. Cargo Reconciliation and Verification

- Arriving cargo should be reconciled against cargo manifests; departing cargo should be verified against purchase or delivery orders. All shortages, overages, and significant discrepancies must be investigated and resolved.

6. Layered Security Strategy

- Implement a layered security approach: establish role-specific protocols for drivers during stops and breaks, use physical security measures (e.g., hard locking devices), and integrate technological solutions such as covert tracking devices and carrier vetting tools. Technology must be properly integrated into existing processes.
- Conduct tabletop exercises twice a year to ensure all personnel understand their roles in responding to theft incidents.

7. Employee Education and Industry Partnerships

- Educate employees about evolving threats, especially phishing attacks targeting passwords and email accounts. Join industry groups and regional security councils to stay informed and strengthen partnerships.

8. Supply Chain Communication

- If a credible threat is detected, alert affected business partners and law enforcement agencies as soon as feasibly possible.

Reporting Suspected Violations

CTPAT members who identify evidence of illegal activity should report it immediately to U.S. Customs and Border Protection (CBP):

- **CBP – Report Suspicious Activity by calling 1-800-BE-ALERT (232-5378)**
- **CTPAT – Report Suspicious Activity to the company's assigned SCSS**



Summary

Cargo theft is a rapidly escalating threat to U.S. supply chains, requiring CTPAT Members to adopt rigorous security procedures, proactive reporting, layered security strategies, and ongoing employee education. Immediate reporting, thorough investigation, and strong industry partnerships are essential to mitigate risks and support recovery efforts.

The best practices identified herein are intended to help industry guard against diversion risk.

Both government and industry recognize that implementing effective import and export compliance programs is an important component of responsible corporate citizenship and good business practices.

CTPAT Program

CBP.GOV/CTPAT

Publication Number: 5496-0326