# STRATEGIC CARGO THEFT PREVENTION

ascot

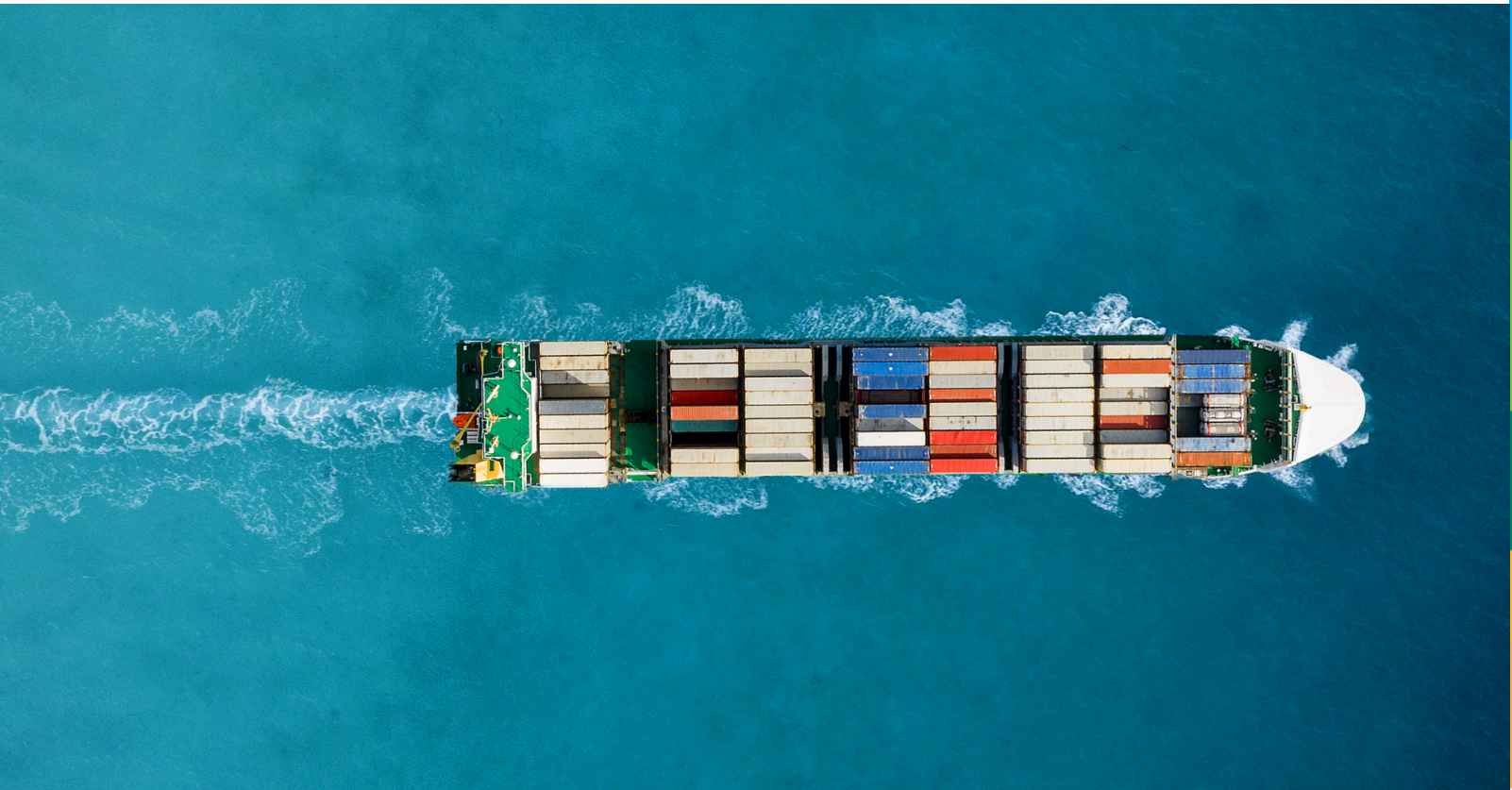
A perfect partner for a less-than-perfect world.™

## LEARN HOW TO HELP PREVENT THIS RAPIDLY INCREASING TYPE OF CARGO THEFT WITH ASCOT LOSS CONTROL

Strategic theft occurs when a cargo load is acquired by thieves through deception or fraud. This may include misleading shippers, brokers, or carriers into giving their load of goods to bad actors instead of to the intended carrier. While technology has gotten more adept at detecting anomalies, thieves have fine-tuned their tactics in tandem.

Strategic thefts typically take place at freight consolidator warehouses. U.S. states with high activity include California, Texas, Florida, Georgia, and Illinois, but strategic thefts have spread to other points and locations throughout the supply chain. Many thieves are staking out warehouse locations to understand what types of goods are coming and going, when, and by whom. They then deploy common tactics including carrier identify theft, bulk purchasing of motor authority credentials, double brokering, and fictitious pick-up schemes (see sidebar on pg. 2 for more information) to acquire the goods. Thieves often target items that can be easily resold including food and beverage, electronics and household goods.

Read on for best practices and procedures to protect your cargo from strategic theft.



- THE TRUCKING INDUSTRY EXPERIENCED LOSSES IN THE RANGE OF $500-$700 MILLION ANNUALLY. (TIA, 2023)
- STRATEGIC THEFTS HAVE INCREASED 68% ACROSS THE U.S. AND CANADA IN THE FOURTH QUARTER OF 2023 AS COMPARED TO THE SAME PERIOD IN 2022. (CARGONET)

Knowing who you are doing business with is the best way to mitigate the risk of strategic cargo thefts. Some key considerations to safeguard your shipments include:

- **Verify Carriers –** Verify the carriers you are working with to ensure that they are legitimate. Obtain information on how long they have been in business, who their other clients are, etc. Resources include the Federal Motor Carrier Safety Administration (FMCSA) and SAFER websites. Verify the identity of the driver and truck details at the time of pickup. The utilization of secure pick-up numbers can also assist in the reduction of strategic types of thefts and ensure that the correct party is receiving the load.

- **Communicate –** Keep lines of communication open between suppliers, brokers, carriers, and your employees. Foster an environment and culture that prioritizes cargo theft prevention and encourages employees and drivers to report concerns. Educate drivers and employees about cargo theft and train them on what to look for and how to report incidents. Educate all parties about the importance of reporting suspicious emails and avoiding phishing attempts.

- **Collaborate –** Work together to ensure that goods are being picked up and delivered by the proper carrier/driver. Collaborate with industry peers, law enforcement, and security professionals to learn more about best practices and evolving tactics being used by cargo thieves.

# A Guide to Common Theft Methods

**Carrier Identify Theft**
Thieves use another motor carrier's assigned USDOT number or act as a broker without proper registration with the FMCSA, typically using information that has been fraudulently obtained (e.g. phishing emails, malware and spoofing domains).

**Double Brokering**
Thieves act as intermediaries between shippers and carriers, gain access to load boards, and redirect a load from the shipper to another carrier without the shipper's knowledge.

**Fictitious Pick-Up Schemes**
Thieves create false documentation in order to convince a supplier or warehouse that they are the intended carrier, collect the cargo, and disappear with the goods.

**13,398 CARGO THEFTS WERE REPORTED IN 2023, VALUED AT OVER $1.32 BILLION DOLLARS (FBI)**

- 3.6% WERE ATTRIBUTED TO FALSE PRETENSES OR SWINDLE
- 1.1% TO IDENTITY THEFT
- 0.5% TO IMPERSONATION
- 0.1% TO HACKING

**OF ALL CARGO STOLEN, ONLY 10.5% WAS RECOVERED**

## *CASE STUDY*

*The Ascot Cargo Claims team has recognized an increasing number of cargo thefts, supporting what is being observed across the transportation industry. A recent claim involved a driver using fraudulent documentation to pick up a load of retail clothing at the designated warehouse location. The trucking company hired to make the pickup had their computer system hacked, and the perpetrators were able to access all shipment information and documentation necessary to present to the warehouse facility to load the product.* ***The thief drove away with over $725K in cargo.*** *Using a carrier with a more secure website and formal cyber security protocols could have potentially prevented this theft. In addition, warehouse personnel should always verify the driver information and truck information on the pickup documentation by checking the driver's license and license plate of the truck. If the license plate or driver's license differ from the paperwork, the warehouse should immediately contact the carrier before tendering the load.*

- **Utilize New Technology –** New and evolving technologies can assist with the tracking of loads and reduce errors at the time of pickup. Monitor cargo movement from origin to destination using GPS, RFID, or other similar technology.

- **Assess Risks –** Criminals and their tactics are always evolving. Conduct regular security assessments. Review physical security, digital/ cyber security, travel routes, and types of goods being shipped and received.

- **Trust Your Instincts –** Finally, if something does not feel "right," trust your instincts and ask more questions before releasing a load.

**Contact David A. Larson, Ascot U.S. Head of Loss Control & Risk Management, to learn more about our loss control capabilities. Visit ascotgroup.com for more information about our Cargo risk solutions.**

**RESOURCE CENTER**

Broker and Carrier Fraud and Identity Theft | FMCSA (dot.gov)
SAFER WEB (dot.gov)
FMCSA Registration | FMCSA (dot.gov)
Report Fraud Hotline | DOT OIG