CLIENT ALERTS & INSIGHTS

Grand Theft Cargo: Practical Ways Freight Brokers Can Avoid Cyber-Enabled Cargo Theft

APRIL 9, 2026

Authors: Nicholas P. Lacey, Christopher J. Letkewicz

Featured Practices: Data Privacy & Cybersecurity

Featured Industries: Transportation & Logistics

Key Takeaways

- Cyber-enabled cargo theft is a modern form of freight theft in which criminals use digital impersonation, stolen credentials and system manipulation to fraudulently obtain cargo, often without ever physically handling it themselves.
- As these schemes become more sophisticated and widespread, they expose freight brokers and shippers to significant financial losses, operational disruption and potential contractual or insurance-related liability.
- Brokers should strengthen carrier vetting and verification protocols, closely examine documentation and communications for inconsistencies, and proactively review insurance coverage and contractual terms to ensure cyber-enabled theft risks are adequately addressed before releasing loads.

What is Cyber-Enabled Cargo Theft?

Cargo theft is not a new phenomenon, but in recent years it has evolved into an increasingly sophisticated, often international enterprise aimed at surreptitiously taking possession of another's freight through calculated fraud and deception. An emerging, tech-driven alternative to straight cargo theft, cyber-enabled cargo theft occurs when fraudsters steal cargo remotely without ever taking physical possession of the cargo, often using identity theft and cyber manipulation to deceive unwary shippers, brokers and carriers. Indeed, as defined by the National Motor Freight Traffic Association, "[c]yber-enabled cargo theft occurs when digital compromise-such as stolen credentials, impersonated email accounts, or manipulated systems-is used to enable physical cargo theft, double brokering, or financial fraud."[1] According to the National Insurance Crime Bureau, cargo theft is a $15 to $35 billion industry in America.[2] The average loss per incident exceeds $250,000 based on recent statistics.[3]

Freight brokers can fall prey to such schemes, which can cause significant business and supply chain disruptions, as well as potential liability.

The Sophisticated Means of Cyber-Enabled Cargo Theft

A common tactic employed by fraudsters in recent years is identity theft-whereby fraudulent actors gain access to a legitimate motor carrier's credentials and use those credentials to book loads through online load boards, including third-party load boards or a broker's own proprietary load board. Trading on a legitimate motor carrier's MC number and using the legitimate motor carrier's login credentials for the load board, the fraudsters are able to bid on and receive loads, often while raising very few red flags. In many cases, the legitimate motor carrier is one who has already been vetted and approved by the broker and completed past loads for the broker without incident. The fraudster directs the driver, who may himself be unwitting to the scheme, to go to the pick-up location, load the cargo and divert it from its intended destination.

Small motor carrier operations without an established data security infrastructure are often more susceptible to the kinds of data breaches that allow fraudulent actors to misappropriate their identities. A compromised email account is a primary feature of fraudulent carrier impersonation. Many of the warning signs are subtle, but with careful scrutiny, they may be uncovered.

Minimizing Cyber-Enabled Cargo Theft

While there is no cure-all to prevent cargo theft, there are steps that freight brokers can take to spot red flags and minimize the potential of releasing a load to a fraudulent actor. Brokers should adhere to the following practices, some of which have been highlighted recently by the Federal Motor Carrier Safety Administration ("FMCSA"),[4] to prevent cyber-enabled cargo theft:

- Confirm that the phone number provided by the carrier matches the phone number posted on the FMCSA's SAFER database:: If the number provided by the carrier does not match the posted number, brokers should call the posted number to confirm whether the legitimate carrier actually booked the load. Clever fraudsters may provide a phone number that is one digit off from the legitimate carrier's number in an effort to go unnoticed. In some cases, a simple phone call can thwart an attempted theft. Even if everything appears to be in order, making a phone call to the carrier's SAFER-posted phone number is a good rule of thumb prior to engaging a motor carrier, particularly for carriers who have not regularly been engaged by the broker.
- Maintain communication with the shipper or its agent who will actually be loading the cargo at the pick-up location: Prior to releasing the cargo to the driver, require the shipper or its agent to photograph the truck's placard and the driver's license to confirm that the name and U.S. DOT number on the placard and the driver's information match the information provided by the carrier. In some cases, simply confirming that this information comports with the information provided by the carrier can prevent cargo theft.
- Closely examine documents: Closely examine bills of lading, rate confirmation and insurance certificates, and verify the accuracy of information through multiple sources, if possible.
- Use extra caution when considering a carrier who does not have a domain-registered email account (e.g., Gmail, Yahoo!): While using such accounts should not be categorically disqualifying, many instances of fraudulent carrier impersonation are perpetrated against carriers who use such accounts, so brokers should consider taking extra precautions when contacted by a carrier without a registered domain name.

Preventing cyber-enabled cargo theft requires implementing security measures and verifying carrier identity before cargo is released to a carrier, as reacting once the cargo has been loaded is usually too little, too late. Although cargo theft has gained the attention of various federal and state law enforcement agencies, it is often very difficult to pin liability on the actual wrongdoer, particularly when it's a foreign actor.

In addition to spotting red flags in order to prevent cargo theft, as last lines of defense, brokers should consider whether their insurance policies and customer-facing contracts sufficiently address cargo theft. While most contingent cargo insurance policies contain exclusions for things such as dishonest acts of the carrier or fraudulent pick-ups, some insurance products offer endorsements for deceptive pickups and cybercrimes. While the federal liability regime under the Carmack Amendment[5] does not impose liability on brokers for lost or stolen cargo, a shipper may require a contractual provision requiring the broker to accept liability as if it were a carrier. If a broker is in a position to reject such a contractual provision, based on the value of the business relationship, they should do so in order to avoid contractual liability for cargo theft.

While cargo theft can't be eliminated entirely, brokers can minimize the likelihood of its occurrence through diligence and thorough vetting procedures.

---

[1] National Motor Freight Traffic Association, Inc., Freight Fraud Prevention Hub. Cyber-Enabled Cargo Theft Explained. https://freightfraudhub.com/fraud-basics/cyber-enabled-cargo-theft/.

[2] National Insurance Crime Bureau. On the Rise: Cargo Theft, a Billion Dollar Industry. https://www.nicb.org/news/blog/rise-cargo-theft-billion-dollar-industry.

[3] Verisk CargoNet. Cargo Theft Losses Surge to Estimated $725 Million in 2025, Verisk CargoNet Analysis Reveals. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2025-theft-trends/.

[4] Federal Motor Carrier Safety Administration. Broker and Carrier Fraud and Identity Theft. https://www.fmcsa.dot.gov/mission/help/broker-and-carrier-fraud-and-identity-theft.

[5] 49 U.S.C. § 14706 (imposing liability for the "actual loss or injury to the property" on a "carrier").