IUMI and TAPA EMEA issue joint warning on fake carrier fraud and cargo crime risks

The International Union of Marine Insurance (IUMI) and the Transported Asset Protection Association (TAPA) EMEA call for urgent action by supply chain stakeholders and government authorities to combat the growing risk of fake carriers and other cargo crime tactics. Fraudulent pickups have particularly impacted supply chains in Europe, North and South America, with violent modus operandi being most prevalent in Africa and Latin America. While it is true that the growth of these types of events in Europe and the US has been alarmingly fast, it is equally true that (albeit more gradually) the same trend is emerging across all regions around the world.

Recent data highlights an alarming trend for cargo theft generally and freight fraud in particular. The losses indicate that cargo crime has moved "from the asphalt to cyberspace", with criminals increasingly using digital tools to conceal their true identities and shift from physical theft and violent hijackings to sophisticated online fraud:

- Cargo theft losses in North America reached USD 455 million in 2024, with over 3,600 reported incidents. The average loss per incident exceeds USD 202,000.[1]
- TAPA EMEA's cargo crime intelligence database recorded over 108,000 thefts from supply chains in more than 110 countries in Europe, the Middle East and Africa in the last two years. The 5% of these crimes reporting their loss value were worth a combined €1 billion+, the equivalent of >€1.3m every 24 hours. Major incidents (€100K+) averaged €878,525.[2]
- Strategic cargo theft and organised crime account for around 18% of all thefts in the US as criminals adopt increasingly sophisticated tactics to attack supply chains.[3]
- "Phantom freight" frauds have surged in Mexico. According to the American Transportation Research Institute (ATRI), this kind of strategic theft skyrocketed (up to 15 times) since 2022. Notorious cases involved stealing high-value shipments (e.g., truckloads of tequila) through fraud, with no violence used.[4]
- The German Insurance Association (GDV) reports a dramatic increase: In the first seven months of 2025 alone, 88 cases of so-called phantom carriers were registered – as many as in the entire previous year. In Germany, a full truckload disappears every three days, resulting in losses of around €18 million by the end of July 2025.[5]

---

[1] 2024 Supply Chain Risk Trends Analysis, Verisk: https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-theft-trends/
[2] TAPA EMEA intelligence service: https://tapaemea.org/incident-service/
[3] Cargo Theft Tactics and Trend Report 2025, Munich Re, 26 March 2025: https://www.munichre.com/specialty/global-markets-uk/en/insights/cargo-and-freight/cargo-theft-tactics-and-trends-report-2025.html
[4] ARM Services: https://arm-services.com/en/home/
[5] 2025 Verschwundene Lkw-Ladungen: Versicherer warnen vor hohen Schäden durch Phantomfrachtführer: https://www.gdv.de/gdv/medien/medieninformationen/verschwundene-lkw-ladungen-versicherer-warnen-vor-hohen-schaeden-durch-phantomfrachtfuehrer-193494

Criminal groups increasingly focus on the fraudulent theft of truck consignments by securing regular freight contracts under false or misused identities. They set up shell companies, hijack or impersonate legitimate firms, or operate under stolen credentials so that, at the point of collection, everything appears to be a normal transport. Once they have taken charge of the goods with the intent to steal them, the contract is not fulfilled. The consignment does not reach its intended recipient and is instead resold elsewhere. By this stage, the ostensible business partner has vanished without a trace.

The method is low risk and high reward because the cargo is handed over voluntarily. Offenders rely on simple but effective digital deception: spoofed or forged email addresses, look-alike domains, fake insurance certificates, and counterfeit driver credentials. Access to freight exchanges or company systems is increasingly obtained by compromising user accounts through phishing, password reuse, or other credential attacks. While AI is not central to current cases, emerging AI tools can streamline document forgery, identity obfuscation, and credential harvesting, making these schemes easier to scale and potentially driving larger losses over time.

It is not only one-off contracts that are affected. Repeat bookings and framework agreements are also targeted, which increases the potential severity of losses.

To counter these worrying global developments, IUMI and TAPA EMEA urge all stakeholders to take joint action as follows:

- To counter fraud, shippers are advised to vet all carriers and drivers continuously. Use only agreed, secure communication channels with continuously vetted contacts. Verify email addresses and phone numbers before each transport order, even in ongoing relationships. Minor changes to contact details are a common fraud tactic.
- Cross-check driver credentials and freight forwarder details.
- Adhere strictly to existing standards such as TAPA's Cyber Security Standard and Freight Broker Security Requirements (FBSR) Standard and GDV's loss prevention guidelines on fraudulent theft of truck consignments (phantom carriers).
- Abnormal behaviours such as unusual routing, last-minute changes, or mismatched contact details are clear warning signs and should trigger precautionary measures.
- Secure parking and route planning remain critical to prevent in-transit theft.
- Use technology to increase the real-time GPS monitoring of fleets.

A crucial element in the fight against cargo fraud are freight exchange platforms. They have a key responsibility to ensure no bogus carriers can operate on the platforms. IUMI and TAPA EMEA encourage these platforms to implement robust identity verification and fraud detection protocols, including multifactor authentication. Their support and cooperation is essential to closing loopholes which are increasingly being exploited by fake carriers.

While fraudulent carriers dominate headlines in Europe and North America, violent theft remains rampant in other regions. Hijackings still account for many cargo theft incidents, with hotspots in Brazil, South Africa, and parts of Europe. At the same time, TAPA EMEA and IUMI aim to raise awareness and mobilize stakeholders and authorities, alerting all players in the global supply chains to this growing challenge. Even if it is not a pressing issue today in some places, it will be one soon given the rapid impact of AI technologies when they are being misused.

IUMI and TAPA EMEA reaffirm their individual commitments to supporting insurers, shippers, logistics providers and freight exchange platforms. Through advocacy, cooperation and best practices, we can work to strengthen supply chain resilience against evolving threats.

For further information contact:

Mike Elsom (IUMI): mike@mikeelsom.com

Jamie Roche (TAPA EMEA): jamie@jamierochepr.co.uk

About IUMI

The International Union of Marine Insurance e.V. (IUMI) is a non-profit association established for the purpose of protecting, safeguarding and advancing insurers‘ interests in marine and all types of transport insurance. It also provides an essential forum to discuss and exchange ideas, information and statistics of common interest for marine underwriters and in exchange with other marine professionals.

IUMI currently represents 42 national and marine market insurance and reinsurance associations.

www.iumi.com

About TAPA EMEA

The Transported Asset Protection Association was founded as a not-for-profit industry Association in 1997 to help Manufacturers/Shippers and their Logistics Service Providers minimize losses from their supply chains resulting from cargo thefts.

www.tapaemea.org