



MSIG
SPECIALTY MARINE



FAKE CARRIERS A GROWING THREAT

CIRCULAR

SEPTEMBER 2026

All Rights Reserved

1. Introduction

Digital transformation continues to reshape the entire supply chain, with the logistics sector being no exception. Elements such as online carrier sourcing, remote onboarding, as well as reliance on digital freight exchanges became standard practice across the industry. While improving efficiency and cutting costs, they also carry new risks.

Fake carrier fraud exploits the weakest link in logistics operations, namely trust. Trust in the process of booking transportation and in the collection of cargo. Criminals posing as legitimate carriers do not need to resort to physically stealing the cargo, instead they present false identities and fraudulent documentation and in turn get the cargo handed over to them. This illicit practice has exponentially grown in scale across Europe in recent years, in Germany alone, a truckload of cargo is reported stolen every three days, with a significant part of it being linked to such phantom carriers.

This circular aims to delve deeper into the matter, raise awareness as well as suggest possible ways to tackle the problem.

2. Definition

A fake carrier or a phantom carrier involves a criminal (organisation) whose modus operandi centres around impersonating a legitimate logistics company and is aimed at illegally taking over cargo from legitimate companies.

The most common forms of this practice would include:

- ◆ Using stolen credentials, e.g. by phishing or data breaches
- ◆ Creating copied and slightly altered company name, domain, branding etc. to manipulate potential victims
- ◆ Using forged certificates of insurance, licence and driver documentation
- ◆ Creating shell transport operators in order to pass due diligence
- ◆ Entirely fictitious companies created for fraudulent purposes

3. Modus operandi

The most effective crimes are often the simplest. Similarly, fake carriers operate in a surprisingly simple way. The main element the criminals need to obtain is an identity to appear to others as a legitimate logistics company. This is mostly achieved by impersonating an existing company either by stealing an existing identity or forging one. With this new identity, the criminals get access to freight exchange platforms, once that threshold is passed, they get access to virtually endless opportunities across the world.

To secure a shipment, phantom carriers offer attractive, yet not 'too-good-to-be-true' pricing and are willing to accommodate urgent requests. Once a shipment is secured, a driver arrives at a collection point with seemingly intact documents. The cargo is released. From this point onwards, the shipment gets diverted, transloaded, often moved across jurisdictions and resold before the crime even gets reported. One of the most striking elements of this practice, often overlooked, is the fact that the cargo itself is handed over to the criminals voluntarily.



4. Phantom carriers on the rise

Based on the data from the German Insurance Association (GDV), 88 cases of fake carrier fraud were reported in 2024, followed by 171 cases in 2025 – almost twice as many. The average loss incurred rose from approx. EUR 130,000 to EUR 180,000 per case, with an entire truckload falling to phantom carriers every second day. The total loss reported in Germany in 2025 amounted to a staggering EUR 30 million.

The increase in Germany is mirrored across the entire continent and is largely attributable to the ease with which one could operate across the online freight exchange platforms. It is these platforms, offering broad, fast and near-anonymous access to the logistics market that are a significant enabling factor in the growth of cargo theft. This is further supported and amplified by phishing, compromised email accounts as well as identity theft.

While no specific type of cargo is off the criminals' radar, the choices they make are not random. The most sought-after types are valuable, resaleable, in high demand and challenging to trace. While the German GDV data points to chemicals, pharmaceutical products and electronics, the renewed Dutch G23 clause was put into place due to the increase in theft of valuable construction materials such as boilers, solar panels and heat pipes.

Other sources mention categories reaching from food and beverage, up to rare metals being targeted. It seems no cargo can truly be safe from this illicit activity.

A recurring pattern visible in Germany and Benelux involves the criminals simply cloning the identity of legitimate, mid-sized companies. They replicate all key details, including insurance certificates, logos, branding etc. and register it on almost identical domains by swapping .nl to .pl or .com. Such slight alterations often manage to bypass checks and do not raise suspicion as legitimate companies often have multiple domains for each country they operate in. It is imperative to stay vigilant at all times. Key red flags allowing to identify such fraudsters include:

- ◆ Look-alike email domains and/or minor spelling changes
- ◆ Reliance on non-corporate email accounts (@gmail.com, @yahoo.com etc.)
- ◆ Requests to move communication outside of the freight platform
- ◆ Recently established or unknown carrier
- ◆ Last-minute changes to carrier, routing or driver
- ◆ Contact details not aligned with official records
- ◆ Insurance certificates, registration documents and transport licences that cannot be independently confirmed
- ◆ An almost surprising ability to accommodate urgent, last-minute requests and changes
- ◆ Mismatched driver and vehicle documentation

5. Exposure, insurance considerations and risk mitigation

Phantom carrier is a form of fraud posing a growing threat across the supply chain. Cargo owners face direct losses, freight forwarders and other actors in the logistics sector face increasing scrutiny and due diligence to differentiate themselves from the criminals. In turn, insurers are confronted with an increase of claims that are not the simplest to handle. From an insurance perspective, there is a growing degree of uncertainty with respect to issuing an adequate policy response. A large part of this uncertainty is attributable to elements such as the voluntary handover element or fraud exclusions. Paired with the fact that recovery remains somewhat limited and that the reliance on freight exchange platforms carries potential accumulation risk, it most definitely remains a conundrum for the industry to tackle.

The use of online freight exchange platforms can have contractual and insurance-related consequences.



The updated Dutch G23 model clause related to theft of cargo during road transport was published in 2025. It contains specific wording related to losses linked to the use of these online freight exchange platforms, including a higher deductible for instances where theft or misappropriation of goods is a consequence of it. This can have a significant impact on carriers.

In response to the challenge ahead, various mitigating measures should be taken:

- ◆ Logistics providers and freight forwarders need to implement robust and 2026-proof carrier onboarding processes, including independent verification with call-back procedures in place
- ◆ Cargo owners need to operate with a heightened duty of care, especially with respect to high-value shipments and aim to build their own network of trusted carriers
- ◆ Warehouse operators should diligently verify each driver, vehicle as well as collection references before releasing the cargo

Across the board, various controls and checks need to be implemented. While commonly used freight exchange platforms have their own safety mechanisms and verification processes, relying on them blindly is highly inadvisable. Before engaging an unknown carrier, cargo interests should conduct their own due diligence checks. This should include verifying their registration details, transport licences, information regarding ownership, and their corporate identifiers such as the Chamber of Commerce registration number or VAT number. Most of these are readily available online. Their insurance credentials are also a giveaway – the insurance certificate, policy number as well as the cover period should also be verified. Aspects such as the identity of the driver, vehicle registration as well as all necessary documentation and references for cargo collection should also be verified prior to cargo release.

With respect to internal controls of the freight exchange platforms, TIMOCOM verifies new users before authorisation, independent document verification has also been put in place. Paired with carrier ratings based on user experience as well as monitoring irregularities. Similarly, Teleroute screens new companies, including company information, licences, as well as insurance information forming

the core of the process. What both companies stress, however, is that there can be no 100% protection against freight crime and that their internal checks are not meant to replace the checks that are their users' own responsibility.

Other resources active in the sector, such as Stichting Fake Carrier (www.fakecarrier.com) can provide invaluable practical theft prevention guides, help with their expertise on carrier verification and raise awareness of the practice itself to boost industry resistance.

Ultimately, phantom carrier fraud is on the rise as a result of a seemingly trustworthy and seamless process. It is largely anonymous and involves multiple steps where each subsequent party relies on the other one. In turn, some end up operating undetected.



6. Conclusion

Fake carrier fraud shows how the criminal world evolves with new technologies and makes use of the new ways of conducting business. It shows how valuable cargo can fall into the hands of criminals without forced entry at night or a roadside attack. In a modern logistics environment, the riskiest moment is in fact when an illicit phantom carrier manages to disguise itself as a legitimate one. Once that point is passed, their seemingly perfect crime gains momentum, often leading to a voluntary release of cargo and individual losses in the hundreds of thousands of euros.

The most effective response available is therefore prevention. What the industry requires is well-trained personnel and robust processes that not only verify all relevant information regarding the carrier, the vehicle, the driver and their insurance details, but also enable the identification of irregularities, red flags and triggers. This verification process needs to be treated as an integral part and core of cargo security. Due diligence, clear accountability and well-trained staff need to become essential to creating an effective defence against this ever evolving and sophisticated threat.

The content of this circular was prepared by MSIG Specialty Marine NV for the addressee and for informational purposes only. This circular is not and is not intended to be construed as an offering, and insurance products or services mentioned might not be available. It does not constitute legal advice. Nothing in this information should be interpreted as providing guidance on any question relating to policy interpretation, underwriting practice, or any other issues in insurance coverage. No warranties are made regarding the thoroughness or accuracy of the information contained in this content, and MSIG Specialty Marine NV is not responsible for any errors or omissions. Use of it is at the user's own risk, and MSIG Specialty Marine NV expressly disclaims all liability with respect to actions taken or not taken based on any contents of it. No rights can be derived from it under any circumstances.



Aleksander Podolak
Contractual Loss Prevention Advisor

+31 10 799 5800

Aleksander.podolak@msigspecialtymarine.com



MSIGSPECIALTYMARINE.COM

MSIG Specialty Marine NV - Registered office at Boulevard du Roi Albert II 37, 1030 Brussels (Belgium) - www.msigspecialtymarine.com

Registration Number BCE 0670.726.393 - Supervisory Authority : Financial Services and Markets Authority ("FSMA") Brussels

Statute : Belgian Mandated Underwriters and Belgian Reinsurance agents

UK branch - The Leadenhall Building 122 Leadenhall Street, London, EC3V 4AG - Registration number of the company Companies House number FC031206 -

Registration Number of the Branch BR016272 - Registered with the Financial Conduct Authority ("FCA") number 985124

MSIG Specialty Marine NV is a member of MS&AD Insurance Group Holdings, Inc.

A member of **MS&AD** INSURANCE GROUP