CLECAT

European Association for Forwarding,
Transport, Logistics and Customs Services

Guide on preventing Identity-Based Cargo Theft

Introduction

Cargo theft remains a significant and evolving risk for the European road transport and logistics sector. While traditional cargo theft involving physical force persists in terms of incident numbers, an increasing proportion of overall financial losses results from deception-based schemes. Criminals increasingly exploit procedural weaknesses, digital communication channels and operational time pressure.

The objective of this guide is to support proportionate preventive actions and controls that reduce exposure and financial losses, while also providing pragmatic guide in the event of an incident. It aims to promote proportionate due diligence standards, reinforce operational verification procedures and enhance resilience against deception-based threats. Above all, the focus is on embedding practical controls into everyday workflows in a way that is realistic, workable and aligned with the operational realities of freight forwarders.

Over the years, national freight forwarding associations, insurers and other stakeholders have developed a wide range of checklists, standards and practical tools to address cargo crime. The aim of this guide is not to duplicate that valuable work, but to consolidate relevant insights, highlight emerging trends in deception-based cargo theft, and support a more structured and proportionate approach to risk mitigation within daily operations.

This guide draws on discussions and exchanges within CLECAT, including contributions from members who have been actively supporting their national communities in strengthening risk management practices. In particular, input and practical experience from the Association of Logistics and Freight Forwarding of the Slovak Republic (ZLZ), the German Freight Forwarding and Logistics Association (DSLV) and the Freight Forwarders Association of Romania (USER) have informed this work. Their engagement and willingness to share lessons learned are gratefully acknowledged.

The measures described are not legally binding and do not replace company-specific risk management procedures. While the guide does not seek to duplicate existing tools, companies may consider translating the guidance into short internal checklists, training materials or customer-specific security arrangements, depending on their structure and risk profile. This may support more consistent and practical implementation of the measures outlined.

Table of Contents

1. Understanding the Cargo Theft Risk Landscape

Cargo theft in road freight transport remains a significant and evolving risk across Europe. While traditional theft involving physical force continues in terms of incident frequency, the financial severity of losses is increasingly driven by deception-based schemes, in particular identity theft and so-called phantom hauliers.

A growing share of high-impact cargo theft cases involves identity-based fraud schemes, often referred to as ''phantom carriers''.

In these cases, criminals establish or impersonate seemingly legitimate transport companies to obtain transport assignments. These entities may present valid registration details and documentation but operate with fraudulent intent.

Such schemes typically rely on a combination of access to operational information (e.g. shipment details, routes, contact data), access to the transport chain (through digital platforms or subcontracting), and the involvement or manipulation of individuals. This combination creates structural vulnerabilities that can be exploited without the use of physical force, making detection more difficult and prevention more dependent on robust procedures and due diligence.

These schemes are inherently difficult to detect at an early stage. In many cases, cargo is voluntarily released to a driver presenting seemingly legitimate documentation, with no visible signs of criminal activity at the loading site. As a result, incidents often only become apparent once the goods fail to reach their destination, significantly reducing the chances of recovery.

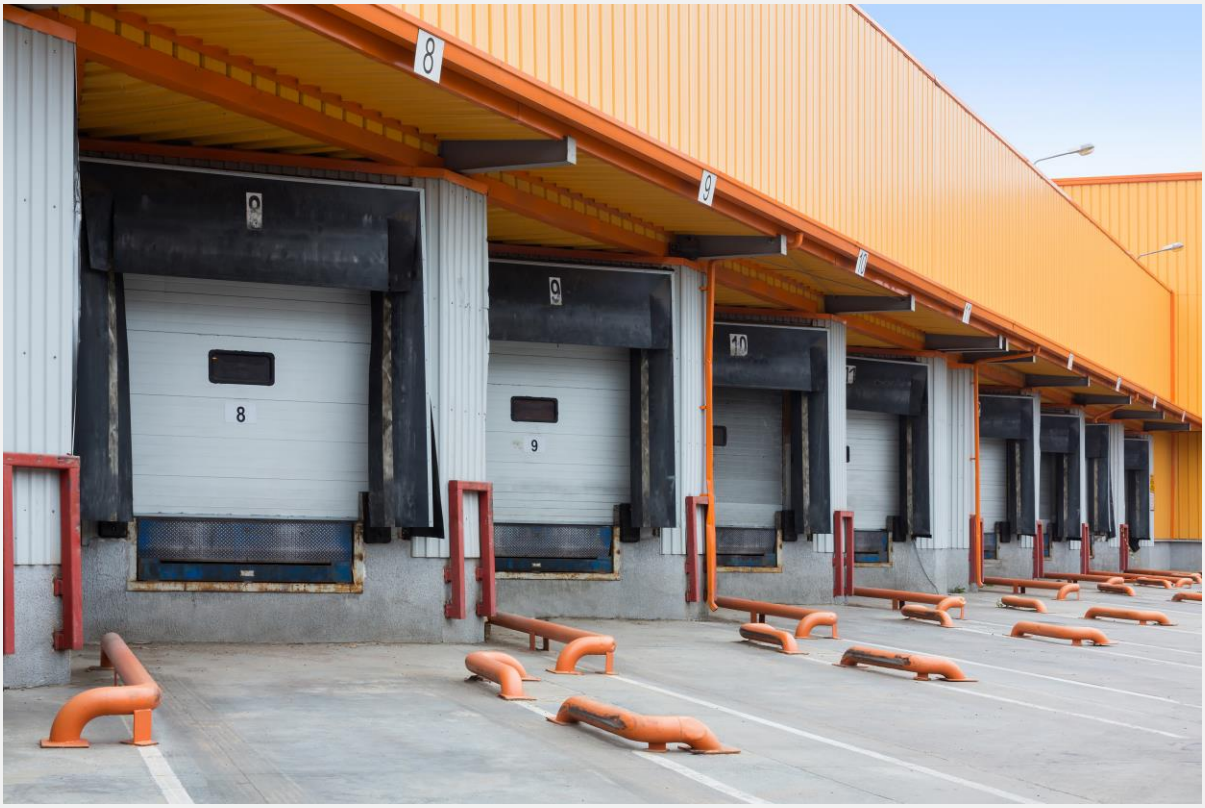
Cargo theft, and in particular identity-based fraud, is not only an operational challenge but a systemic risk to supply chain integrity. Effective prevention therefore cannot rest with freight forwarders alone. It requires coordinated action across the supply chain, involving also parties like the shippers. While freight forwarders play a central role in carrier selection and operational control, shippers also have a clear responsibility in mitigating risks, through transparent communication and due diligence.

In a cross-border context, it is important to note that the legal qualification of a party as a freight forwarder or as a carrier may differ between Member State jurisdictions. A company that is considered to have contracted purely as a freight forwarder under the law of one Member State may, under the law of another, be more readily qualified as a carrier or principal contractor.

Depending on the applicable national legal framework, such qualification may have implications for liability exposure and insurance coverage in cases involving fraudulent or “phantom” carriers. In some jurisdictions, qualification as a carrier may result in broader liability exposure, including, in certain circumstances, the possibility of unlimited liability. Insurance implications may also arise, for example where freight forwarders are not insured for certain forms of carrier liability or where different deductibles apply. Operators should therefore be aware that contractual roles may be interpreted or requalified differently across borders, potentially affecting liability exposure and insurance arrangements in the event of cargo theft.

A further challenge is that the scale and nature of the problem remain difficult to quantify. Reliable EU-wide statistics on cargo theft remain limited. In many Member States, police reporting systems do not systematically distinguish between different types of theft, such as cargo theft, vehicle theft, or fraud involving so-called phantom carriers. Incidents may therefore be initially classified as fraud or contractual disputes rather than organised cargo theft. This can delay coordinated law-enforcement responses and complicate cross-border investigations. As a result, national authorities often lack a complete overview of fraud patterns. This fragmentation complicates risk assessment, enforcement coordination and recovery efforts.

Industry stakeholders and insurers therefore widely consider existing figures to represent only a partial picture, with a significant share of incidents remaining unreported or not properly classified. Nevertheless, available data illustrate the magnitude of the threat. According to figures presented by the German Insurance Association (GDV), during the first seven months of 2025 alone, 88 cases involving phantom hauliers were registered in Germany, equalling the total recorded during the entire previous year. While these figures refer to one national market, industry stakeholders report similar trends across other European countries, reflecting the increasingly cross-border nature of organised cargo theft.



2. Increasing Financial Severity and Insurance Exposure

The financial exposure associated with deception-based cargo theft has increased significantly in recent years. Under the Convention on the Contract for the International Carriage of Goods by Road (CMR), the party that concludes the contract of carriage with the shipper is considered the carrier and is therefore responsible for the transport of the goods. In practice, freight forwarders frequently organise transport in their own name and therefore act as contractual carriers, even when the physical transport is carried out by a subcontracted road carrier. In such cases, the forwarder remains responsible towards the customer under CMR, while the subcontracted carrier acts as the performing carrier within the contractual chain.

Insurers are therefore increasingly scrutinising whether adequate due diligence was performed when appointing carriers or subcontractors. In cases involving shell companies, identity fraud or insufficient verification procedures, insurers may examine whether appropriate checks, controls and contractual safeguards were applied before determining the scope of coverage.

Additional complexity arises in fraud cases where the goods never enter a legitimate transport operation. This may occur, for example, when criminals impersonate carriers and divert shipments before the transport begins. In such cases, insurers may question whether the incident falls within the scope of transport liability regimes such as CMR, which can further complicate recovery of losses.

Smaller transport operators may face increasing difficulty in obtaining liability insurance with sufficiently high coverage limits for high-value transport. Freight forwarders should therefore not only verify the existence of insurance certificates but also assess whether the scope of coverage and insured limits are appropriate in relation to the value and risk profile of the cargo being transported.

Cargo theft should therefore not be viewed solely as an operational disruption. It represents a material financial and governance risk that can directly affect a company's balance sheet, risk management obligations and long-term competitiveness.

2.1 Evolution of Criminal Modus Operandi

The threat landscape in cargo theft has evolved in recent years, shifting from opportunistic physical theft to increasingly structured and professionalised identity-based fraud. Analysis presented by DSLV and German law enforcement (Polizei Borken, 2025) shows that criminal groups increasingly rely on deception and identity manipulation rather than direct physical intervention. Common modus operandi includes the establishment of shell transport companies that operate legitimately for one or two years before being used for fraudulent activities, the acquisition of existing transport companies whose identities are subsequently misused, and the hijacking of legitimate transport or freight exchange accounts through phishing or hacking. In other cases, criminals present forged licence plates, driver licences or registration documents during the cargo pick-up process or arrange transport under false client identities before diverting the goods after loading.

Current assessments suggest that approximately three quarters of phantom haulier cases involve identity theft rather than purely fictitious companies. These schemes are typically well organised, digitally enabled

and increasingly international in nature. Criminal actors frequently use freight exchanges for reconnaissance, credibility building and the targeted acquisition of transport contracts.

Several structural characteristics of modern logistics operations further increase the vulnerability of supply chains to such deception-based schemes. The extensive use of digital booking and communication platforms, fragmented subcontracting structures, cross-border carrier networks and remote onboarding procedures create an environment where verification often takes place without direct physical interaction. At the same time, operational time pressure and the frequent need for last-minute capacity sourcing can reduce the level of scrutiny applied when selecting a carrier.

Freight exchanges play an important role in enabling operational flexibility and efficient capacity allocation within European logistics networks. However, they also lower entry barriers for malicious actors. Most freight exchange platforms assume no liability for fraud incidents, and some recommend limiting the placement of high-value cargo on such platforms above certain thresholds. The combination of digital interaction limited physical contact, and commercial urgency creates a risk environment in which minor anomalies may easily be overlooked.

While these platforms provide essential operational flexibility, industry associations and insurers increasingly highlight the need for stronger identity verification mechanisms, including robust onboarding procedures, continuous monitoring of user accounts and multi-factor authentication. Strengthening platform-level controls can significantly reduce opportunities for fraudulent actors to misuse stolen identities or operate shell companies within digital freight marketplaces.

2.2 Challenges in Detection and Investigation

Fraudulent transport theft is often difficult to detect immediately because the cargo is voluntarily released to a driver presenting what appears to be legitimate documentation. Unlike traditional cargo theft involving forced entry, there are typically no visible signs of criminal activity at the loading site.

As a result, incidents are sometimes initially classified as cases of fraud or contractual disputes rather than organised cargo theft. This can delay coordinated law-enforcement responses and complicate cross-border investigations. Many of these cases involve organised criminal networks capable of rapidly storing, redistributing and reselling stolen goods through secondary markets. For this reason, early reporting and accurate documentation of suspicious circumstances at the loading site are critical for effective investigation and recovery efforts.

Cargo theft statistics across Europe remain fragmented because incidents often involve multiple jurisdictions. A shipment may be loaded in one Member State, subcontracted through a company in another Member State and reported to law enforcement in a third jurisdiction. As a result, national authorities often lack a complete overview of fraud patterns. This fragmentation complicates risk assessment, enforcement coordination and recovery efforts.

2.3 Key Commodities Targeted by Organised Cargo Theft

Criminal groups generally focus on goods that combine high value density, strong secondary market demand and ease of resale. Such products can be quickly redistributed through parallel markets, making them particularly attractive targets for organised cargo theft. Commonly targeted commodities include:

- electronics and consumer technology.
- pharmaceuticals and medical products.
- luxury goods and branded fashion.
- high-value retail and consumer products.
- alcohol and tobacco.

The attractiveness of these goods is often linked to their high resale value, limited traceability and strong demand in secondary markets. Therefore, freight forwarders should apply heightened vigilance and enhanced verification procedures when handling shipments involving such commodities. Shipments involving these commodities should normally trigger enhanced due diligence procedures as outlined in the following section.

2.4 Examples of Deception-Based Cargo Theft

Case Example 1: Identity theft of a Known Carrier

A freight forwarder assigned a transport order for consumer electronics through a freight exchange platform. The selected carrier presented documentation identical to that of a well-known transport company operating in another Member State. The criminals had copied the legitimate company's licence, insurance certificate and branding, but used a slightly altered email domain.

At pickup, the vehicle and driver appeared legitimate and the cargo was released without further verification. The shipment never reached the consignee and was later discovered to have been diverted and resold.

To mitigate this risk, it is advisable to agree on transport order details via the freight exchange's internal messaging system and only subsequently confirm them by email. Communication through secured platform environments, generally provides a higher level of traceability and reduces the risk of impersonation, whereas creating fraudulent email accounts that closely resemble legitimate carriers remains relatively easy for criminals.

Case Example 2: Dormant Company Used for Fraud

A company registered two years earlier began accepting small shipments through freight exchanges and completed several legitimate transports. However, after accepting a high-value pharmaceutical shipment, the company disappeared following the pickup of the cargo.

It was later discovered that the company had no real assets and ceased operations immediately after the fraud. This case example demonstrates that operational history alone does not fully eliminate risk, and

that high-value shipments require additional verification even dealing with apparently established partners. To mitigate this risk, it is recommended to place transport orders only with carriers that demonstrate a consistent history of activity on freight exchanges, supported by a sufficient number of positive reviews. Carriers that have been active for at least one to two years and have accumulated several verified positive reviews, which lowers the risk of cargo loss.

Case Example 3: Vehicle Substitution at Pickup

A driver arrived with documentation matching the transport order but presented a different trailer type than specified. The loading site did not verify the Vehicle Identification Number (VIN) or trailer details and released the cargo. The vehicle was later found to have been rented under false identification and abandoned after cargo diversion. In this case, the vehicle configuration mismatches and last-minute changes must always lead to enhanced verification before loading the cargo.

Case Example 4: Licence Plate Substitution at Loading

Industry reports highlight cases where vehicles arriving for loading do not match the licence plates communicated in the transport order. In several incidents reported in countries such as Romania or Spain, trucks arrived with different registration numbers than those previously confirmed. After loading, the vehicles disappeared with the cargo.

This scheme often involves the use of licence plate numbers belonging to legitimate transport companies whose identities are misused to gain credibility. If staff at the loading site do not verify that the arriving vehicle matches the information in the transport order, the cargo may be released to a fraudulent carrier. To mitigate this risk, it is important to verify the vehicle registration number and carrier's identity before releasing the goods.

3. Risk-Based Due Diligence Framework

Cargo theft rarely results from a single failure. Losses typically arise from a sequence of procedural gaps, such as incomplete carrier validation, overlooked inconsistencies in company information, insufficient driver or vehicle checks at loading, or acceptance of unauthorised changes to transport or delivery instructions. Cargo theft prevention should therefore not rely on isolated controls, but they must be embedded within daily workflows so that verification and mitigation mechanisms operate systematically. This is time consuming and requires staff and resources which is sometimes lacking or there are urgencies.

Enhanced due diligence should be applied when risk increases, including:

3.1 First-time cooperation / recently established carriers

A limited operational track record makes it more difficult for freight forwarders to assess the reliability and credibility of a newly established company. For this reason, enhanced due diligence is essential when a new market entrant submits a quotation for high-value, theft-sensitive or otherwise atypical cargo movements.

Such checks may include verifying company registration details, VAT status, management information and the validity and scope of insurance coverage. Additional vigilance is recommended where a newly established carrier offers to transport high-value cargo at unusually low or highly competitive rates, as this may signal elevated risk.

3.2 High-value shipments

Risk exposure varies significantly according to value density, commodity attractiveness, ease of resale, shipment traceability and route risk profiles. Electronics, pharmaceuticals, branded consumer goods and high-demand retail products remain particularly attractive targets. For this reason, increase vigilance is recommended when handling high-value shipments, engaging new carriers, managing last-minute operational changes or executing cross-border movements.

Internal procedure should be established for high-value shipment or high-risk transports while ensuring that the selection of a carrier is reviewed by more than one staff member.

3.3 Operational urgency

Time pressure is a common tactic used by fraudsters and criminal networks to circumvent established due diligence controls. By creating a sense of urgency, they seek to limit scrutiny and accelerate decision-making before proper verification can take place.

Requests such as “immediate loading required,” “vehicle already at the gate,” or “urgent replacement due to breakdown” should never justify bypassing established verification procedures. Driver identity, vehicle details, transport documentation and carrier credentials must continue to be checked in line with internal controls.

4. Carrier Selection and Verification

Carrier selection is a key risk control. Assigning cargo without adequate verification significantly increases exposure.

4.1 Legal and Registration Verification

Freight forwarders should verify:

- Legal entity registration
- Company registration number and status
- Valid VAT number
- Community licence or transport authorisation
- Ownership or recent management changes

Registration data should be cross-checked against official registries. Even minor inconsistencies should trigger clarification before cargo assignment, while dormant or recently reactivated entities require particular attention.

4.2 Insurance Verification

Liability insurance verification is both a fraud-prevention and financial-risk control.

Verification should include:

- Identity of the insurer
- Validity period
- Geographical scope
- Coverage limits relative to cargo value
- Proof of insurance premium payment, such a recent payment confirmation

Independent confirmation with the insurer is recommended for high-value shipments.

Risk indicators include:

- Recently issued certificates without history
- Altered formatting or inconsistent documentation
- Refusal to allow insurer verification

4.3 Internal Vulnerabilities and Information Exposure

Identity-based cargo theft schemes may also rely on access to internal information or the manipulation of operational staff. Sensitive information such as shipment details, planning data or customer contacts can be exploited if not adequately protected. Organisations should therefore ensure that access to such

information is limited to a need-to-know basis and that employees are aware of social engineering risks, including unsolicited requests for operational data.

4.4 Summary of Warning Indicators for Identity-Based Cargo Theft

The following indicators, particularly when combined, may signal an elevated risk of fraudulent transport arrangements:

Company-related indicators

- Newly established companies with limited or unverifiable operational history
- Lack of online presence or only a basic / recently created website
- Use of generic email domains (e.g. Gmail, Hotmail) instead of corporate addresses
- Inconsistent or incomplete company registration, VAT or insurance information

Communication-related indicators

- Requests received through unusual communication channels or outside normal procedures
- Pressure to act quickly or bypass standard verification steps
- Changes in contact details, bank information or carrier identity during the process

Shipment-related indicators

- High-value or theft-sensitive goods combined with unusually attractive pricing
- Vague, inconsistent or incomplete cargo descriptions
- Discrepancies between the nature of goods and the delivery location

Operational indicators

- Last-minute changes to pick-up or delivery instructions
- Requests for additional stops or route changes without clear justification
- Delivery locations that do not correspond to expected business activities

The presence of one indicator does not necessarily imply fraud. However, multiple indicators should trigger enhanced verification procedures.

As a practical rule, the presence of one serious inconsistency, or several smaller anomalies, should lead to the suspension of cargo release until verification has been completed by a designated responsible function. This would further support operational decision-making, particularly for loading-site personnel, reinforcing the principle that verification controls should not be bypassed.

5. Secured Digital Communication

Digital communication channels are among the most frequently exploited entry points for identity-based transport fraud. Criminals often impersonate legitimate carriers by using email domains that closely resemble genuine company addresses. The differences are typically minor, for example, a single altered character, and can easily go unnoticed in fast-paced operational environments where staff work under time pressure.

Communication verification should therefore be treated as a core security control, ensuring that instructions originate from the genuine contractual carrier and not from an impersonator. Where possible, multi-factor authentication and secure document-sharing environments should be introduced to reduce the risk of unauthorised account access.

Freight forwarders should in particular:

5.1 Compare sender email with verified records

The sender's email address should be checked against previously verified company records. While some legitimate operators may use public email domains, their use in newly established business relationships or high-value cargo increases uncertainty and justifies enhanced verification.

5.2 Verify telephone contact details

Freight forwarders should not rely solely on telephone numbers provided in incoming emails. Instead, contact details should be retrieved from trusted and independently verified sources.

5.3 Confirm critical instructions via alternative channels

Unusual requests, changes to delivery details, or amendments to banking information should always be confirmed through an independently verified communication channel. This is especially important when dealing with newly established carriers, high-value cargo or time-sensitive transactions. Communication verification must be treated as a core security control.

6. Financial Safeguards

Payment diversion frequently accompanies identity-based fraud.

Financial due diligence should include:

- Matching IBAN to legal entity name
- Verifying country consistency
- Confirming banking changes via independently validated contact channels

Banking detail changes must never be accepted solely by email confirmation.

7. Loading Site Controls

The loading site is the final checkpoints in the transport chain because once cargo has been released and the vehicle has departed, the ability of a freight forwarder to intervene, redirect, or recover goods becomes limited. For this reason, verifying the driver identity must be a standardised operational practice applied consistently, especially for high cargo value.

In this context, it is important to recognise the specific role of loading site personnel. The individual at the loading site is often not the person who selected or contracted the carrier yet is ultimately responsible for the physical release of the goods. They should therefore be equipped with simple, operationally usable decision tools and clear procedures, including the explicit authority to stop loading and escalate where inconsistencies or warning signs arise. Strengthening this aspect would further enhance the practical effectiveness of loading-site controls.

7.1 Driver Verification

Before release of cargo:

- Inspect national ID or passport: The document should be valid, undamaged, and free from visible signs of alteration. Attention should be paid to photograph edges and surface irregularities.
- Verify driving licence validity and category.
- Compare physical appearance with document photograph.
- Confirm consistency with transport documentation.

Refusal to cooperate with reasonable verification demands should be treated as a significant risk indicator.

7.2 Vehicle and Equipment Verification

Vehicle manipulation is a frequent fraud method. For example, criminals may present substituted vehicles, stolen or cloned registration numbers, falsified registration documents, or short-term rentals intended to limit traceability and hinder post-incident investigations.

Since licence plates are relatively easy to copy or replace, having in place verification procedures that extend beyond simple plate recording is paramount, as a comprehensive validation process significantly reduces the likelihood of releasing cargo to unauthorised operators.

Freight forwarders should verify:

- Vehicle registration number (format and authenticity).
- Registration certificate consistency.
- VIN where suspicion arises:
- Unexpected vehicle configurations (e.g. curtain-sider instead of refrigerated unit) that may signal substitution or operational irregularities.
- Vehicle suitability for cargo type.
- Both tractor and trailer identifiers.

Cross-checking registration against insurance records strengthens control.

All verification steps should be documented and comply with data protection requirements.

8. Incident Response Protocol

Despite preventive measures, incidents may occur. In such cases, immediate actions should include:

- Notification of law enforcement
- Notification of insurer
- Suspension of related movements or payments
- Informing contractual partners

Evidence preservation is critical. Freight forwarders should:

- Secure and preserve all relevant documentation, including contracts, transport orders, CMR consignment notes and identification records.
- Retain digital evidence such as email correspondence, telephone records and system access logs.
- Document the timeline of events.

Following the immediate response phase, a structured internal review should be conducted. This should include a root-cause analysis to identify procedural gaps and an assessment of whether due diligence measures were correctly applied.

9. Continuous Improvement and Staff Awareness

Cargo theft mitigation depends on consistent application of controls. Freight forwarders should therefore:

- Provide staff training on risk indicators
- Conduct periodic internal reviews
- Update procedures in response to new fraud patterns

Most importantly, verification procedures must be embedded in daily operations rather than applied on an ad hoc basis.

10. Conclusion

Cargo theft in road freight transport increasingly relies on deception, identity theft and procedural weaknesses. In this evolving environment, prevention depends less on isolated controls and more on systematic due diligence as part of daily operations.

This guidance provides freight forwarders and logistics service providers with a set of measures aimed at reducing exposure through proportionate due diligence, strengthened verification procedures, secured communication practices and reinforced on-site controls.

Implementation of these measures can enhance resilience across the supply chain. It is equally important to respond effectively when incidents occur, through timely reporting, documentation preservation, cooperation with insurers and authorities, and continuous improvement of internal procedures.

Effective cargo theft mitigation depends on consistent application of controls, with preventive measures that must be embedded in standard operational processes rather than applied on an ad hoc basis. When verification standards are applied systematically and risk indicators are addressed without delay, freight forwarders can materially reduce financial exposure, limit operational disruption and strengthen the overall integrity of cross-border logistics operations within the EU.

Cargo theft increasingly operates across borders and often exploits regulatory fragmentation, digital identity weaknesses and gaps in cross-border enforcement. Strengthened cooperation between freight forwarders, carriers, shippers, insurers, digital freight platforms and law enforcement authorities will therefore remain essential to improving prevention and investigation.