

## Fake Carriers Avoidance Guidance Document

# V<sub>1</sub>

Trucking Security Requirements  
Guidance Document for users  
of TAPA Standards

**TAPA EMEA**  
Kanaalpark 140  
2321 JV Leiden  
The Netherlands

**[www.tapaemea.org](http://www.tapaemea.org)**  
**[info@tapaemea.org](mailto:info@tapaemea.org)**



## Table of Contents

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| 1. Introduction.....                                                               | 3  |
| 1.1 Purpose and Scope .....                                                        | 3  |
| 1.2 Who this guide is for .....                                                    | 3  |
| 2. The Fake Carrier Threat.....                                                    | 4  |
| 2.1 Common schemes.....                                                            | 4  |
| 2.2 Transportation Subcontracting Platforms .....                                  | 8  |
| 2.3 FTL vs. LTL and Groupage specific risks .....                                  | 9  |
| 3. Red Flags & Warning Signs.....                                                  | 11 |
| 3.1 At Onboarding and Vetting .....                                                | 11 |
| Example 1: The Lookalike Domain .....                                              | 12 |
| Example 2: The Country-Code Switch .....                                           | 12 |
| Example 3: Examples of ID Theft Attempts.....                                      | 13 |
| 3.2 At Booking and During Communication.....                                       | 18 |
| 3.3 At the Point of Collection .....                                               | 18 |
| 3.4 Recycle of assets and resources used in known past frauds. ....                | 19 |
| 4. Carrier Vetting & Onboarding / Ongoing Monitoring & Operational Safeguards..... | 19 |
| 5. Legal & Contractual Protections.....                                            | 20 |
| 5.1 Key contract clauses and liability considerations.....                         | 20 |
| 5.2 Insurance Coverage Gaps.....                                                   | 20 |
| 6. Summary.....                                                                    | 22 |
| ANNEX A – Basic Checklist .....                                                    | 24 |

# 1. Introduction

## 1.1 Purpose and Scope

This document provides practical guidance to help organizations identify, prevent, and respond to the risk of engaging with fraudulent or “fake” carriers within the transportation and logistics sector. The increasing sophistication of schemes and number of cargo theft, identity theft, and digital fraud has made it more difficult to distinguish legitimate carriers from malicious actors. As a result, robust due diligence, verification processes, risk awareness, and response protocols are essential across the supply chain.

The purpose of this guide is to:

- Raise awareness of the methods used by fake carriers and associated criminal networks
- Outline common warning signs and risk indicators in carrier selection and load tendering processes
- Recommend preventive measures and verification procedures to reduce exposure to fraud
- Provide guidance on response actions in the event of suspected or confirmed incidents

The scope of this document covers road freight operations and related logistics activities, including carrier selection/onboarding, load assignment, subcontracting practices, and communication protocols. While the focus is on preventing fake carrier fraud, many of the principles outlined are applicable to broader cargo security and supply chain risk management practices.

## 1.2 Who this guide is for

This guide is intended for all stakeholders involved in the planning, procurement, and execution of freight transportation and logistics services. It is particularly relevant for:

- **Shippers and Manufacturers** (i.e., Procurement, Security, and Quality/Compliance Teams) responsible for tendering freight, selecting transport providers, and involved in carrier vetting, risk management, and suppliers’ management/governance.
- **Logistics Service Providers (LSPs)**, including freight forwarders, brokers, and third-party logistics (3PL/4PL/5PL) companies managing carrier networks.
- **Carriers and Transport Operators** seeking to protect their identity, assets, and reputation from fraudulent misuse.
- **Operations and Customer Service Personnel** engaged in day-to-day shipment planning, communication, and execution.

## 2. The Fake Carrier Threat

### 2.1 Common schemes

The threat posed by fake or fraudulent carriers has grown significantly in recent years, driven by the digitalization of freight procurement and the increasing complexity of logistics networks. Understanding the most common schemes is the first step toward effective prevention.

- **Double Brokering:** Double brokering is one of the most prevalent and difficult-to-detect forms of carrier fraud in modern supply chains. In its basic form, it occurs when a carrier or broker that has been awarded a load by a shipper, re-tenders that load — without authorization — to another carrier. The shipper believes they are dealing with a single, vetted party, while in reality the cargo is being handled by an entirely different operator who has no contractual relationship with the shipper and may never have been vetted at all.

What makes double brokering particularly insidious is that it does not always result in immediate cargo loss. In many cases, the freight is delivered — late, damaged, incomplete, or without proper documentation — and the shipper only discovers the fraud when filing a claim and finding that the carrier named on the bill of lading has no knowledge of the shipment. Insurance coverage gaps are a common consequence, as the actual hauler may carry insufficient or fraudulent insurance, leaving the shipper exposed.

In more predatory forms, double brokering is used deliberately as a setup for cargo theft. The fraudulent intermediary selects a load, re-brokers it to an accomplice posing as a legitimate carrier or even to a legitimate carrier who doesn't know he is part of the scheme, and the cargo is subsequently diverted and stolen. These schemes are often run by organized groups that operate multiple fictitious carrier entities simultaneously, cycling through them to avoid detection.

Double brokering is facilitated by several market conditions: the competitive pressure on rates that incentivizes carriers to accept more loads than they can handle, the widespread use of open load boards with minimal verification, and the speed of digital freight transactions that leaves little room for manual oversight. Shippers and brokers who rely solely on upfront carrier vetting — without monitoring subcontracting activity during execution — are particularly vulnerable.

- **Identity Cloning:** Identity cloning represents a more calculated and technically sophisticated form of carrier fraud. The perpetrator does not invent a fictitious company from scratch; instead, they systematically steal and replicate the identity of a real, established carrier — one with a clean losses/claims record, active authority, and valid insurance — and use that stolen identity to deceive shippers and brokers into awarding them loads.

The mechanics of identity cloning in the EMEA region typically follow a recognizable pattern. Fraudsters identify a legitimate carrier through publicly accessible national and European registries. These include national company registers as well as operator license databases maintained by national transport authorities. In the broader EMEA context, fraudsters may also exploit the relative inconsistency in registry accessibility and data quality across markets — targeting carriers registered in jurisdictions where public records are more easily extracted or less frequently updated.

From these sources, fraudsters extract the carrier's legal company name, registered address, VAT number, national operator license number, and Community License details where applicable. They then produce fraudulent documentation replicating these credentials, including forged CMR consignment note headers, carrier onboarding packets, certificates of insurance, and VAT registration confirmations, altering only the contact details — email address, telephone number, and bank account information — so that all communications and payments are redirected to themselves.

In more elaborate cases, fraudsters build convincing replica websites that mirror the legitimate carrier's online presence, including fleet photographs, route maps, and company history. They may register lookalike domains that closely resemble the real carrier's web address — substituting characters, adding hyphens, or using country-code top-level domains different from the original (for example, using a .com domain to impersonate a carrier whose legitimate site is .de or .fr) — to pass cursory inspection by procurement or operations teams. In cross-border EMEA scenarios, the use of a different country domain can even appear plausible, as many genuine carriers operate internationally.

The multi-jurisdictional nature of EMEA logistics creates additional opportunities for identity cloning to go undetected. A carrier legitimately registered in Poland, Romania, or Bulgaria — countries that supply a large share of international road haulage capacity across the continent — may be less familiar to a procurement team based in Western Europe, making it harder to distinguish a cloned identity from a genuine but unfamiliar operator. Language barriers, differences in document formats across countries, and the sheer volume of cross-border carrier relationships managed by large logistics operations all work in the fraudster's favor.

The legitimate carrier is typically unaware that their identity is being exploited until they begin receiving complaints about shipments they never performed, disputes over invoices they never issued, or contact from law enforcement or insurers. Meanwhile, the shipper who believed they were working with a trusted operator has suffered cargo loss and faces complex, cross-border legal and insurance challenges in seeking recourse — particularly when the fraud has involved carriers or bank accounts registered across multiple jurisdictions.

Identity cloning exploits a fundamental weakness in carrier vetting: the tendency to verify credentials once — at onboarding — rather than on a continuous basis. A

carrier that passed all compliance checks several months ago may have had their identity cloned in the interim, and without re-verification at the point of each new booking or periodic review cycle, the fraud can persist undetected across multiple shipments.

- **Fictitious Carriers:** While identity cloning involves stealing an existing carrier's identity, fictitious carrier fraud involves the creation of entirely fabricated carrier entities. Fraudsters register new carrier authorities — often with minimal scrutiny in jurisdictions with light-touch registration requirements — establish a superficially credible online presence and begin soliciting or accepting loads before the carrier has any operational history that would trigger suspicion.

Fictitious carriers are often distinguished by certain common characteristics:

- very recent authority registration dates,
- no verifiable operating history or references,
- insurance certificates from obscure or unverifiable underwriters,
- minimal or generic online presence,
- and contact information that traces to virtual offices or prepaid mobile numbers.

They may offer unusually competitive rates to win loads quickly, knowing that their window of operation before detection is limited.

These entities are frequently disposable — used for one or a small number of fraudulent pickups before being abandoned, with the perpetrators moving on to a new fictitious identity. This "**burn and rotate**" model makes them difficult to pursue through traditional fraud investigation channels.

- **Account Takeover (ATO)** is a sophisticated cargo theft scheme in which bad actors illicitly gain control of a legitimate carrier's established account on load boards and freight marketplaces, or broker proprietary platforms. Rather than creating a fraudulent entity from scratch — a method increasingly flagged by vetting systems — these criminals exploit the hard-won reputation and compliance credentials of real, operating carriers.

The scheme typically begins with **credential harvesting**: fraudsters obtain login details through phishing emails targeting carrier dispatchers or owner-operators, credential stuffing attacks using leaked username/password combinations from unrelated data breaches, or by purchasing stolen credentials on dark web marketplaces. In some cases, insiders or former employees provide access directly.

Once inside the account, the bad actor **silently assumes control**, often changing contact phone numbers, email addresses, and banking/payment details while leaving the carrier's license number, insurance certificates, and security scores

intact and visible to brokers. This is deliberate — the fraudulent operator now presents a clean compliance profile they did not earn.

The actor then **books loads aggressively**, targeting high-value, time-sensitive freight — electronics, pharmaceuticals, food-grade cargo — through the compromised account. When contacted by the broker for confirmation, they impersonate the legitimate carrier's dispatching team. At pickup, a truck bearing cloned or replicated placards and sometimes counterfeit Bill of Lading documentation arrives at the shipper's dock. The freight is loaded and vanishes into a shadow network of warehouses or is immediately transshipped.

By the time the **legitimate carrier** discovers the breach — often triggered by missed payment inquiries or shipper complaints — the load has long disappeared, leaving brokers, shippers, and insurers to absorb significant losses.

- **Business Buyout** is a cargo theft scheme closely related to Account Takeover fraud — both can be seen as two variations of the same underlying strategy of parasitizing an existing, legitimate carrier identity rather than building a fraudulent one from scratch. Where Account Takeover relies on credential theft and hacking to seize control of an active carrier's platform presence, the Business Buyout exploits the legal transfer of business ownership itself as the entry point. Criminal actors acquire — through outright purchase or forged change-of-ownership paperwork — a **legitimate, dormant, or distressed trucking company** that holds an established authority approval, operating licenses, and operational history. Fraudsters specifically target small carriers that are financially struggling, recently inactive, or whose aging owner-operators are looking to exit the industry. The acquisition may involve a nominal cash payment, assumption of debts, or in some cases simply filing falsified documentation, effectively hijacking the company's regulatory identity without the original owner's knowledge or consent.

Once in control of the carrier entity, the criminal operation **activates the dormant company** and rapidly re-enters the freight market, presenting an apparently seasoned carrier with years of operating history, existing insurance certificates, and a clean safety record — all of which pass standard broker vetting checks with ease. They register on major load boards, establish relationships with multiple brokers simultaneously, and begin booking high-value loads at scale before any red flags emerge. The tell-tale signs are often subtle at first: a sudden spike in booking volume from a previously low-activity carrier, recently updated contact details and banking information, or drivers whose behavior at pickup does not match an experienced carrier's operational norms. By the time the fraud is detected, the criminal group has typically executed multiple theft runs and dissolved their operational footprint, leaving behind only the hollowed-out shell of what was once a legitimate trucking business.

While double brokering, identity cloning, and the use of fictitious carriers are distinct schemes with their own mechanics and warning signs, they frequently share a common end goal: **gaining unlawful physical possession of cargo**. In many documented cases, these schemes are not isolated acts of fraud but deliberate steps in a premeditated theft operation, where the fraudulent procurement of a load is simply the means by which criminal actors obtain access to a shipper's goods. The methods by which cargo is subsequently diverted, stolen, or misdelivered — and the specific commodities, corridors, and seasonal patterns that attract the highest risk — are addressed below.

No discussion of fake carrier schemes is complete without acknowledging the role of insider threat. A significant proportion of sophisticated cargo fraud involves some degree of collusion between external criminal actors and individuals within the shippers', forwarders', or logistics providers' organizations. Insiders may provide shipment manifests, customer data, access credentials, or advance notice of high-value loads in exchange for financial compensation.

Insider involvement dramatically increases the effectiveness of external fraud schemes — it bypasses vetting controls, provides intelligence that makes impersonation more convincing, and delays detection by suppressing internal alerts. Organizations should treat insider threat as an integral part of their fake carrier risk framework, implementing appropriate segregation of duties, access controls, and anomaly monitoring alongside their external carrier vetting procedures.

These schemes are often not mutually exclusive — a single fraud event may combine identity cloning with double brokering before culminating in cargo theft.

## 2.2 Transportation Subcontracting Platforms

The rise of digital freight platforms, load boards, and online subcontracting marketplaces has fundamentally changed how carriers are discovered, vetted, and engaged. While these platforms offer efficiency and market reach, they also introduce significant exposure to fraudulent actors if not used with appropriate controls.

- **Load boards and freight marketplaces** allow carriers to self-register with minimal verification. Fraudulent operators can create profiles using stolen or fabricated credentials, making them appear legitimate to buyers who rely solely on platform-provided data. The speed at which loads are awarded on these platforms — often within minutes — leaves little time for thorough due diligence.
- **Subcontracting chains** represent another area of risk. When a contracted carrier subcontracts to a second or third party through a platform, visibility over who is actually performing the transport is lost. Each link in the chain reduces accountability and increases the risk that the final operator has not been vetted by the original shipper.

**Key risks associated with transportation subcontracting platforms include:**

- Lack of direct contractual relationship between shipper and actual hauler
- Inconsistent or absent re-vetting when a carrier's details change
- Platforms with weak Know Your Carrier (KYC) processes
- Automated load matching that prioritizes speed over compliance
- Difficulty tracing liability in the event of loss or damage

Organizations should establish clear policies if platforms are approved for use, and if yes, what verification steps must be completed before a carrier is onboarded from a platform, and whether subcontracting beyond the first tier is permitted at all. Platform usage should be treated as an extension of the carrier onboarding process, not a shortcut around it.

Another way to control the use of subcontracting platforms is to put a threshold on cargo value, over which use of platforms is not allowed.

## 2.3 FTL vs. LTL and Groupage specific risks

The risk profile of fake carrier fraud varies meaningfully depending on the shipment type. Full Truckload (FTL), Less-than-Truckload (LTL), and groupage (consolidated) shipments each present distinct vulnerabilities that supply chain teams should understand.

- **Full Truckload (FTL)** shipments are the most common target for organized cargo theft schemes, especially under Identity Theft MO. Because a single truck carries one shipper's goods exclusively, a successful interception yields a high-value, homogeneous load that is easier to offload and sell. FTL shipments also tend to involve direct carrier engagement — often through spot procurement — which creates more opportunities for fraudulent operators to insert themselves into the booking process. The risk is heightened when loads are booked under time pressure, during peak seasons, or in lanes where carrier capacity is tight.
- **Less-than-Truckload (LTL)** shipments are generally considered lower-risk for outright cargo theft due to the mixed nature of the load, but they are not immune. Fake carriers, especially under “Account Take-over MO, operating in LTL networks can engage in selective theft — removing specific parts, boxes, parcels or pallets from a consolidated load — which may go undetected for longer than an FTL theft. Identity fraud and double brokering also occur in LTL markets, particularly where regional carriers are engaged on an ad hoc basis and vetting processes are less rigorous than for primary carriers.
- **Groupage and Consolidation Services** introduce a layered risk because multiple shippers' goods are combined into a single transport unit, often passing through multiple handling points and intermediaries. The consolidation process itself — particularly when performed by third-party logistics providers or freight forwarders using spot carriers for the linehaul — can obscure who is handling the cargo at any given moment. Fraudulent actors may infiltrate groupage operations by posing as

legitimate consolidators or by intercepting cargo at a depot or cross-dock point. The mixture of goods from different shippers also complicates liability attribution in the event of loss.

**In all shipment types, risk is amplified when:**

- Carriers are engaged for the first time without a formal onboarding process.
- Bookings are made outside of approved carrier lists or contracted panels.
- Load details (pickup location, cargo description, delivery address) are communicated through unsecured or informal channels.
- Real-time tracking and proof-of-delivery requirements are not enforced.
- Last minute changes in transportation plan/schedule.
- Urgent situations that appear unexpectedly in the operations. In this case, a best practice would be to work with known and trusted parties.
- And of course, whenever the standardized process is violated, in general.

## 3. Red Flags & Warning Signs

Fraudulent carriers rarely display a single warning sign in isolation — it is typically a combination of indicators that should trigger escalation. The following red flags are grouped by the stage at which they are most likely to surface.

Risk assessment should always consider the combination of indicators, the value of the cargo, and the degree to which the carrier relationship has been independently verified. When doubt exists, the default procedure should always be to **pause, escalate, and verify** rather than proceed and assume.

### 3.1 At Onboarding and Vetting

- **Recently issued operating licenses with no verifiable track record.** Legitimate carriers build their business over time; an entity that appears fully formed overnight warrants scrutiny.
- **Credentials that do not withstand independent verification.** Any discrepancy between carrier-provided details and official registry records — company name, license numbers, VAT registration, or Community License details — is a serious red flag.
- **Unverifiable insurance certificates.** Documents referencing obscure underwriters, or policies the insurer cannot confirm, are strong indicators of fraud.
- **Contact details inconsistent with registered information.** Use of free email domains, unregistered phone numbers, or addresses that are slightly changed or differ from official records suggest the carrier identity has been cloned or fabricated.
- **Bank account details in a different country or name.** Payment instructions that do not precisely match the carrier's registered legal entity should always be queried before any load is awarded.
- **Cyber-Enabled Identity Manipulation: Spoofed Domains and Contact Fraud.** A critical enabler of both Account Takeover and Business Buyout schemes is the fraudster's ability to manipulate or spoof the contact details associated with a carrier's identity, making their communications appear indistinguishable from those of the legitimate business they are impersonating. The most common technique is domain spoofing, where criminals register lookalike domain names mimicking the legitimate carrier's web address — swapping letters, adding hyphens, or substituting country-code top-level domains such as .de, .pl, .fr, or .nl to lend geographic credibility across specific European transport corridors. All subsequent communications — spot rate offers, CMR confirmations, and driver check-in messages — are then conducted from the fraudulent domain. Fraudsters further

reinforce the illusion by deploying VoIP virtual numbers with local country codes and by cloning carrier websites entirely, sometimes listing fabricated VAT numbers or falsified license details to pass compliance checks. Taken together, these techniques form a coordinated digital facade that underscores the need to verify carrier identity through authoritative sources such as national transport authority registries or official VAT and company registration records, rather than relying solely on communicated contact details.

#### Example 1: The Lookalike Domain

A well-established refrigerated transport company, **Company Name Transport**, operates under the domain **companyname-transport.eu** and is a trusted carrier on a major European freight marketplace. A criminal group registers the domain **companyname-transports.eu** — adding the letter "s" in their domain name — and clones the company's website entirely, replicating its fleet photos, contact page, and VAT number with a single digit altered. They then approach a Dutch freight forwarder via email offering competitive rates on a high-value pharmaceutical load moving from Warsaw to Amsterdam. The freight forwarder, recognizing the familiar company name and seeing a professional website, books the load. The cargo is collected and never delivered. Only when the forwarder contacts the real Company Name Transport to chase the delivery does the fraud come to light.

#### Example 2: The Country-Code Switch

A legitimate logistics company, **Fast and Fake Log Ltd.**, operates under **fastandfakelog.com** and holds a valid Euro License. Fraudsters register **fastandfakelog.eu** and set up a VoIP number with a local country code to further mimic the genuine operator. They register on a freight exchange platform using the cloned credentials and begin booking groupage loads across the Germany–Romania corridor — a busy and familiar lane that raises no suspicion. When freight forwarders call to confirm bookings, a fluent native-speaking operator answers using the VoIP line, providing convincing dispatch information including fabricated CMR details and driver names. Several loads are successfully stolen across multiple bookings before the pattern is identified by the platform's fraud monitoring team.

### Example 3: Examples of ID Theft Attempts

Please look out for the following names used / abused by fake carriers in some examples simulating new fraud cases:

| Correct                        | Fake                                    | Type of Manipulation                                         | What the employee should notice                                                                             |
|--------------------------------|-----------------------------------------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| info@markus-trans.example      | info@ <b>r</b> markus-trans.example     | Character substitution ("rn" used instead of "m")            | The domain contains "rn" where the legitimate address contains "m". Read the domain character by character. |
| info@codrut-master.example     | info@codrut- <b>r</b> master.example    | Character substitution ("rn" used instead of "m")            | The sequence "rn" can visually resemble "m" in some fonts.                                                  |
| info@tapa-logistik.example     | info@tapa-logisti <b>c</b> .example     | Character substitution / spelling change ("k" → "c")         | The domain name is almost identical, but the spelling has changed.                                          |
| info@markus-kargo.example      | info@markus- <b>c</b> argo.example      | Character substitution ("k" → "c")                           | A single letter has been changed while the overall domain remains plausible.                                |
| user01@codrut-trans.example    | user01@codrut-tran <b>z</b> .example    | Character substitution ("s" → "z")                           | One character has been changed to create a visually plausible domain.                                       |
| user02@tapa-transporte.example | user02@tapa-transport <b>s</b> .example | Spelling variation / character substitution                  | The domain differs by only a small spelling change.                                                         |
| info@markus-logistik.example   | info@ <b>r</b> markus-logistik.example  | Look-alike character / character substitution ("rn" vs. "m") | The suspicious domain may be overlooked because "rn" can resemble "m".                                      |

| Correct                          | Fake                                      | Type of Manipulation                                         | What the employee should notice                                                             |
|----------------------------------|-------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| dispo@codrut-spedition.example   | dispo@codrut-spedit <b>l</b> tion.example | Look-alike character ("l" used instead of "i")               | The lowercase "l" can be mistaken for "i" in some fonts.                                    |
| info@tapa-spedition.example      | info@tapa-spedit <b>l</b> on.example      | Look-alike character ("l" used instead of "i")               | Compare the suspicious domain directly with the known-good domain.                          |
| info@markus-beispiel.example     | info@markus-beispi <b>e</b> i.example     | Character substitution ("i" used instead of "l")             | The final character has changed from "l" to "i".                                            |
| dispo@codrut-spedition.example   | dispo@codrut-spedit <b>ı</b> tion.example | Unicode look-alike / accented character ("ı" instead of "i") | A visually similar accented character is used. Do not rely only on visual appearance.       |
| user03@tapa-logistics.example    | user03@tapa-log <b>ı</b> stics.example    | Unicode look-alike / modified character                      | The "g" contains a dot and is a different Unicode character.                                |
| info@markus-trucking.example     | info@ma <b>e</b> rkus-trucking.example    | Character insertion / spelling manipulation                  | The legitimate company name has been altered by inserting an additional character sequence. |
| info@codrut-kurierdienst.example | info@codrut-kui <b>r</b> erdienst.example | Transposed characters                                        | Two characters have changed position.                                                       |
| info@tapa-falia.example          | info@tapaf <b>a</b> ila.example           | Transposed characters / altered word structure               | The word structure has been rearranged to create a similar-looking address.                 |
| info@markeslink.example          | info@mark <b>a</b> slink.example          | Character substitution ("e" → "a")                           | Only one character differs from the legitimate domain.                                      |

| Correct                            | Fake                              | Type of Manipulation               | What the employee should notice                                |
|------------------------------------|-----------------------------------|------------------------------------|----------------------------------------------------------------|
| info@codrutmann.example            | info@codruimann.example           | Character substitution ("t" → "i") | A single character has been replaced.                          |
| info@tapa-trans.example            | info@tapo-trans.example           | Character substitution ("a" → "o") | One character in the company name has been changed.            |
| info@markusncargologistics.example | info@markuscargologistics.example | Character omission                 | A character has been removed from the legitimate domain.       |
| user04@codrut-transporte.example   | user04@codrut-transport.example   | Character omission                 | The suspicious domain is missing the final letter "e".         |
| info@tapa-european.example         | info@tapaeuropean.example         | Hyphen omission                    | The hyphen has been removed, creating a different domain.      |
| user05@codrut-trans.example        | user05@codruttrans.example        | Hyphen omission                    | The domain looks plausible but the separator has been removed. |
| user06@tapa-gruppe.example         | user06@tapa--gruppe.example       | Additional hyphen                  | An extra hyphen has been inserted.                             |
| info@markus-transport.example      | info@markus-transport.s.example   | Character insertion ("s" added)    | A single extra character changes the domain.                   |
| info@codruttransport.example       | info@codruttransports.example     | Character insertion ("s" added)    | An additional character has been appended to the company name. |

| Correct                              | Fake                                    | Type of Manipulation                                  | What the employee should notice                                                                                 |
|--------------------------------------|-----------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| user07@tapa-trans.example            | user07@tapatrans.example                | Hyphen omission                                       | The domain has been changed by removing the separator.                                                          |
| info@markus.example                  | info@markus-pl.example                  | Additional domain label / misleading suffix           | The suspicious address adds an extra domain label that may appear geographically or organizationally plausible. |
| dispo@codrut.example                 | dispo@codrut.co.example                 | Additional domain label / misleading TLD-like element | The added ".co" may look like a legitimate country or commercial domain element.                                |
| office@tapa-sondertransporte.example | office@tapa-sondertransporte-at.example | Domain suffix manipulation                            | The suspicious address adds a country-like suffix to make the domain appear local.                              |
| user08@markus-route.example          | user08@markus-route-de.example          | Domain suffix manipulation                            | The added "-de" can make the address appear associated with Germany.                                            |
| user09@codrut.example                | user09@codrut-logistics.example         | Additional domain name / impersonation                | A legitimate-looking business term has been added to create a separate domain.                                  |
| user10@tapa-group.example            | user10@tapa-group-lt.example            | Country-code impersonation / suffix manipulation      | The added "lt" may be interpreted as a country reference.                                                       |

| Correct                             | Fake                           | Type of Manipulation                                       | What the employee should notice                                                                         |
|-------------------------------------|--------------------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Markus.transport@example.com        | markus.transport@gmail.com     | Switch to generic email provider                           | A generic mailbox does not prove that the sender represents the claimed company. Verify independently.  |
| codrut-kran@example.com             | codrutcargo2009@gmail.com      | Switch to generic email provider / unrelated mailbox       | The address uses a public email provider and an unrelated-looking mailbox name.                         |
| vorname.name@tapa-transport.example | tapa.transport@gmail.com       | Switch to generic email provider / changed mailbox         | The sender has moved from a company domain to a generic provider. Treat this as a verification trigger. |
| markus-transport.example            | markus.au2@gmail.com           | Switch to generic email provider / minor mailbox variation | A small change in a public mailbox can be difficult to notice.                                          |
| codrut-transport@example.com        | codrut.transportfido@gmail.com | Switch to generic email provider / changed mailbox         | The mailbox name may look personal or plausible but does not establish company identity.                |

## 3.2 At Booking and During Communication

- **Unsolicited approaches with unusually low rates.** Competitive pricing alone is not evidence of fraud, but it becomes significant when combined with other warning signs.
- **Pressure to book quickly or bypass standard procedures.** Artificial urgency is designed to compress time available for due diligence. Any carrier that resists standard vetting should be treated with suspicion.
- **Last-minute changes to agreed details.** Requests to alter pickup time or location, delivery address, driver details, or bank account information shortly before or after booking confirmation are among the most reliable indicators of fictitious pickup or payment fraud.
- **Use of informal communication channels.** Conducting bookings or exchanging load details via personal mobile numbers or messaging apps rather than traceable business channels is irregular and warrants caution.
- **Inability to provide real-time tracking.** A carrier unwilling or unable to share functional GPS visibility — standard practice across EMEA today — should be regarded with suspicion.
- **Change of booking behavior/volume.** Significant increase of bookings within a very small period of time.

## 3.3 At the Point of Collection

- **Driver or vehicle details do not match pre-advised information.** Any mismatch in driver identity, vehicle registration, or trailer type should prevent cargo release pending verification.
- **Driver unable to provide required documentation.** Failure to present a valid CMR, driver's license, or booking confirmation is an immediate cause for escalation.
- **Driver unfamiliar with basic shipment details.** A driver who cannot confirm the cargo description, delivery destination, or consignee details may be operating on behalf of a fraudulent intermediary.
- **Unannounced arrival or significant deviation from the agreed time window.** Criminals executing fictitious pickups rely on busy loading dock staff releasing cargo to anyone who appears to know enough about the shipment.

### 3.4 Recycle of assets and resources used in known past frauds.

A further warning sign that is easily overlooked is the reuse of physical assets across newly formed carrier entities. Criminal groups frequently dissolve a compromised company and re-emerge under a fresh corporate identity yet continue to operate the same tractors and trailers they used before. As a result, a brand-new company with no track record may be running vehicles whose license plates have already appeared in earlier theft or fraud incidents. Because vetting tends to focus on the company's credentials rather than its equipment, this connection often goes unnoticed. Organizations should therefore extend their due diligence beyond corporate and licensing data to the vehicles themselves — cross-checking tractor and trailer registration plates against internal and/or external incident records. A newly registered carrier presenting vehicles with a history of involvement in past incidents is a strong indicator that an old fraudulent operation has simply been repackaged under a new name.

## 4. Carrier Vetting & Onboarding / Ongoing Monitoring & Operational Safeguards

Selecting and onboarding subcontracted carriers is a critical step in maintaining service quality, legal compliance, and liability protection within any freight or logistics operation. Before engaging a carrier, brokers and shippers must conduct thorough due diligence to confirm that prospective partners meet all regulatory requirements and operational standards.

In the [TAPA EMEA Subcontracting Guidance Document](#) the essential procedures for carrier vetting and onboarding are outlined, covering the key verification steps and data sources used to assess carrier reliability, the checks required to validate insurance coverage and operating authority, and a structured onboarding checklist to ensure a consistent and compliant intake process. There is also a very helpful **List of Topics that should be addressed when subcontracting TAPA TSR transports**, that provides a guidance what topics to review when using carriers.

Furthermore, there is a section covering *Escalation and Remediation Procedures in case of Security Incidents*, that provides guidance in:

1. Incident Response, and

## 2. Non-Compliance Response

aiming to address important activities in case of such incidents.

# 5. Legal & Contractual Protections

## 5.1 Key contract clauses and liability considerations

When subcontracting freight operations, the written agreement between broker and carrier serves as the primary line of defense against fraud and misrepresentation. Contracts should explicitly:

1. Prohibit unauthorized re-brokering or double-brokering of loads,
2. Require the carrier to provide immediate notice of any change in operating authority or insurance status, and
3. Include clear indemnification clauses that assign liability in the event of cargo loss, damage, or third-party claims.

To guard against fake or shell carriers, agreements should also mandate that the carrier named in the contract is the entity physically performing the transport, with strict penalties — including immediate termination and financial recovery rights — for any violation. A well-drafted contract does not eliminate risk, but it establishes accountability and provides enforceable remedies when fraud occurs.

## 5.2 Insurance Coverage Gaps

Another very common vulnerability in carrier vetting is the assumption that a valid certificate of insurance is sufficient proof of active, adequate coverage. Fake or high-risk carriers may present certificates that are outdated, fraudulently altered, or issued under policies that have since lapsed or been cancelled.

Brokers and shippers should verify coverage directly with the insurer or through an approved third-party monitoring service, rather than relying solely on documents provided by the carrier. Particular attention should be paid to gaps such as:

1. Insufficient cargo liability limits,
2. Excluded commodity types, or
3. Policies that do not cover the specific lanes or modes of transport involved.

Continuous certificate monitoring — rather than a one-time check at onboarding — is essential to ensure that coverage remains valid throughout the duration of the carrier relationship.

TAPA Copyright © Do Not Copy

## 6. Summary

The fake carrier threat has become a structural risk in modern freight, spanning double brokering, fictitious carriers, identity cloning, account takeover, and business buyout. Though each scheme has its own mechanics, they share a single objective — gaining unlawful access to cargo by impersonating a trusted operator — and are rarely used in isolation. Three themes recur throughout this document:

- fraud thrives in the gap between one-time onboarding and ongoing reality,
- digital platforms and multi-tier subcontracting erode visibility and control over who is actually moving the goods,
- the human element, particularly insider collusion, can quietly defeat otherwise strong controls.

No contract or insurance certificate is self-validating, and no single safeguard is sufficient. Effective protection depends on layered, defense-in-depth controls.

In practical terms, organizations should:

- verify carrier identity against authoritative national and European registries rather than the contact details, websites, or documents supplied by the carrier,
- treat that verification as continuous — repeated at each new booking and on a defined cycle — rather than as a one-off check.

Insurance should be confirmed directly with the insurer (even though sometimes this is time consuming) and monitored over time, and clear policies should govern the use of load boards and the extent of permitted subcontracting, including value thresholds above which platform sourcing is not allowed.

Warning signs should be assessed in combination rather than individually, point-of-collection checks should be strictly enforced, and contracts should prohibit unauthorized re-brokering, name the entity that must physically perform the transport, and carry meaningful penalties for breach.

Insider risk should be addressed explicitly through segregation of duties and anomaly monitoring, and staff should be empowered to pause, escalate, and verify whenever something does not add up.

By treating fake carrier prevention as an ongoing, organization-wide discipline rather than a procurement formality — and by considering practices like the [TAPA EMEA Subcontracting](#)

[Guidance Document](#) and its supporting checklists — stakeholders may significantly reduce their exposure to fraud and strengthen the integrity of the wider supply chain.

Annex A of this document sets out a basic checklist of recommended controls for subcontracted transport, which you can use to reduce your exposure to fake carriers and double brokering.

TAPA Copyright © Do Not Copy

## ANNEX A – Basic Checklist

Where a manufacturer permits transportation subcontracting, the following measures are strongly recommended as a minimum. Any additional controls will depend on risk appetite and load value and are for the sender to decide. These are:

1. LSPs contract with subcontractors under all security requirements set out in this document, and no onward (second-tier) subcontracting is permitted, unless this is explicitly approved by the manufacturer. This is the single most important safeguard against double brokering.
2. Open internet freight platforms should not be used to source subcontracted capacity, as they make carrier identity difficult or impossible to verify, unless there are clear and strict policies related to their approval.
3. LSPs should maintain a current list of all subcontractors used for the customer's goods and make it available on request.
4. Subcontractors should have an established working relationship with the LSP before being used — as a guide, at least 3 months, extended to 6 months for high value goods.
5. LSPs should be able to provide evidence of on-site security audits of their subcontractors and should provide audit reports to the customer on request.
6. LSPs should ensure that only authorized drivers, tractors, and trailers — whether their own or a subcontractor's — are used to transport the customer's goods.
7. LSPs should keep an up-to-date list of all qualified and trained drivers (own and subcontracted) assigned to vehicles in the vehicle register and provide it to the manufacturer on request.
8. All vehicles used should be recorded in the LSP's/applicant's Vehicle Register, ideally capturing tractor and trailer identification, TSR level – if applicable, audit and inspection dates, and any non-conformances and corrective actions. Where the manufacturer operates a Transport Management System, LSPs should be ready to share or upload the register to it on request.

## **Publishing and Copyright Information**

This document is published by the Transported Asset Protection Association (TAPA EMEA Region).

© TAPA EMEA 2026

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted in any form or by any means - electronic, mechanical, photocopying, recording, or otherwise - without prior written permission from TAPA, except as permitted under applicable copyright legislation.

The copyright notice displayed in this document indicates the year in which the document was last issued.

## **Publication history**

First published in September 2026.

The present edition (V1) was published in September 2026.

## **Status of this Document**

This document represents the TAPA EMEA Fake Carriers Avoidance Guidance Document.

The document remains valid until it is replaced, revised, or withdrawn by TAPA EMEA.

TAPA may issue future revisions, updates, or amendments to reflect evolving security threats, industry practices, and technological developments.

## **Use of this Document**

TAPA EMEA does not represent or warrant that the information contained in this document will prevent any loss, damage, or injury to a person or property, because of burglary, theft, hold-up, fire, or other cause, or that information will in all cases provide the protection for which it is intended. If the readers choose to use any information in this document, they assume all the risk and liability for doing so.