

VIGILANT

FRAUD FAILINGS

Fintech and banking got burned by fraudsters. Can logistics learn their lesson before the regulators step in?



BENEFITS BUILT ON CONTINUOUS GROWTH



At TAPA EMEA, we focus a lot on growing our membership.

It's not to make us feel good, it's to help us deliver more benefits to our members. More members = more resources = more we can deliver.

Plus, the bigger we are, the more our influence grows in the eyes of those we want to connect with, such as government ministries, regulatory bodies, other associations, and law enforcement agencies.

A clear example of these growth benefits is the number of events we have been able to offer our members in the past year. In Q4 last year, we organised *Regional Conferences* in France and Romania, and, in 2026, as well as our biggest-ever *Annual Conference* in Germany, our calendar of events has already included conferences in Poland and Sweden (Scandinavia), and, in the coming months, we will also bring together supply chain, security, insurance, and law enforcement stakeholders in Portugal, Spain, and the United Kingdom, as well as members in South Africa.

Every event is a tremendous amount of work, but facilitating industry engagement and connections is a fundamental purpose of TAPA EMEA. We are fortunate that our reach is also greatly supported by our highly committed and totally TAPARIZED Regional Leads. In this issue of *Vigilant*, ahead of hosting our *UK Freight Crime Risk & Resilience Conference*, Harry Hughes

reflects on his first 12 months as UK Regional Lead. Harry has covered a lot of ground representing TAPA EMEA and I am sure his insights will resonate with so many of the TAPA EMEA Family.

We rely on your support

Of course, while we can organise events, we rely on you registering for them and showing up on the day to participate. The level of attendance is always a key measure of whether we see sufficient interest for future events in each specific country. So, please use the links in this issue to **register now**.

And another tangible sign of the value of our growth is the continuous advancement of our TAPA Intelligence System (TIS), which is about to be lifted again with the launch of TAPATRON, your TIS AI Assistant. I encourage you to join our *TIS Deep Dive* webinar on 16 September to see this in action.

And, as we continue to grow, we can say confidently that more will come.



TAPA EMEA
THORSTEN NEUMANN
President &
CEO, TAPA EMEA

CONTENTS



PAGE 3

Meet TAPATRON, your new TIS AI Assistant

PAGE 5

See the latest 17 companies in 12 countries joining the TAPA EMEA network

PAGES 6-9

Fraud: Fintech learned the hard way. Will logistics learn the lesson?

PAGES 10-11

1,077 freight crimes reported to TIS in July in 53 countries with losses exceeding €22.4m or €725,448 every 24 hours as major crimes average €492,351

PAGE 12

Join TAPA EMEA and the Association of Security Directors Portugal (ADSP) in Lisbon on 30 September 2026

PAGE 14

Register now for TAPA EMEA's *Spain Regional Conference* in Madrid on 21 October 2026

PAGES 16-17

Freight exchanges: When security rules block access to secure capacity

PAGES 18-23

Freight crime in the UK – momentum is building but needs to move faster

PAGE 25

Registration closing soon for TAPA EMEA's *UK Freight Crime Risk & Resilience Conference* on 22 October 2026

PAGES 26-27

Standards' FAQs discusses fence heights, walking distances, high value cages, and FSR 2026 and TSR 2026 training courses

PAGES 28-29

See the latest 70 TAPA FSR, TSR & PSR Standards' certifications and PPD partnerships in 20 countries

TAPA EMEA LAUNCHES THE LATEST ADVANCEMENT TO THE TAPA INTELLIGENCE SYSTEM – YOUR TAPATRON AI ASSISTANT



PLAY VIDEO >

The first phase of TAPATRON AI goes 'live' on 1 September 2026 to support TAPA EMEA members' supply chain security.

TAPATRON's AI functionality will help members quickly find and analyse information within our TAPA Intelligence System (TIS) by simply asking questions in natural language. Members can use it for a range of purposes, including:

- **Route planning** – obtaining relevant information to support route planning and risk assessment
- **Cargo crime analysis** – exploring incidents, trends, and relevant crime data
- **Incident searches** – finding incidents based on a particular country or other specific criteria
- **TAPA FSR-Certified locations** – identifying certified locations in a particular country or area
- **Metrics and insights** – retrieving specific information and metrics from the TIS database without having to manually navigate through different sections of the tool

"We are delighted to be launching the next TIS innovation with the help of TAPATRON and the advancements in AI technologies. We believe this latest update will make TIS an even more powerful, efficient, and valuable intelligence tool for our members and provide even greater support to their supply chain security. More will come in the future," said Thorsten Neumann, TAPA EMEA's President & CEO.

Please note that there is a financial limit set internally by TAPA EMEA for each member's usage of the AI tool, and once a member reaches this limit TAPATRON will notify them directly.

Join our next TIS Deep Dive webinar to learn more

Subject: From Reactive to Predictive: Fighting Cargo Crime with AI: Introducing TAPATRON AI & Latest TIS Enhancements

Date & Time:
Wednesday, 16 September 2026 -
10:00–10:45hrs CET

Platform: Microsoft Teams

Webinar Agenda...

1. TAPATRON – Your AI Assistant

We'll explore the role of TAPATRON as your AI Assistant, demonstrate its capabilities, discuss practical use cases, and explain how it will help you access intelligence more efficiently to support faster, more informed security decision-making.

2. Using TIS in your preferred local language

We'll show you how to navigate and use TIS in your preferred language, making the platform more accessible for teams operating across different markets.

3. Resilience Route Planning

Explore the latest enhancements to the Map & Routing module, including the new Resilience Route Planning capability.

4. Latest TIS Enhancements

We'll take you on a practical walkthrough of the newest TIS developments to reinforce how the system is continuing to evolve to strengthen your day-to-day security and supply chain operations.

5. Live Q&A

Our TIS Team experts will be live online to answer your questions.

Whether you rely on TIS every day or are looking to unlock more of its capabilities to support your supply chain security programme, this webinar will provide valuable insights into the platform's latest evolution, developments, and AI-powered intelligence.

SEE TEAMS INVITE IN YOUR INBOX...



TOTALLY TAPARIZED

TAPA EMEA's President & CEO, Thorsten Neumann, shares his personal updates and views on the latest activities aimed at delivering more benefits to the Association's biggest-ever membership network and takes a look at other news and events impacting cargo security and supply chain resilience across our region...



WE HAVE A VERY BUSY TIME COMING UP... AND MORE GREAT BENEFITS COMING YOUR WAY

The peak summer vacation period is coming to a close, and TAPA EMEA members have a lot to look forward to in the coming months.

We have some significant developments coming up between now and the end of 2026:

- Launch of our FSR 2026 & TSR 2026 Standards Trainings, which you can book from 1 September
- Launch of our revised 2026 versions of the TAPA Facility Security Requirements (FSR) and Trucking Security Requirements (TSR), which go 'live' in our Europe, Middle East & Africa region on schedule on 15 September 2026
- Launch of our new TAPATRON TIS AI Assistant and other new benefits as we roll-out TIS 2.0 to give members even greater benefits when using the TAPA Intelligence System as part of your supply chain security programmes
- A joint one-day conference organised by ADSP, the national association of security directors and professionals in Portugal, in Lisbon on 30 September, with all presentations in Portuguese
- TAPA EMEA's local language *Spain Regional Conference* in Madrid on 21 October



- Our *UK Freight Crime Risk & Resilience Conference* in Coventry on 22 October, supported by the British International Freight Association (BIFA) and the Road Haulage Association (RHA)
- Plans to bring members together in South Africa to look at how we can gather more freight crime intelligence, grow our membership, and increase the uptake of the TAPA Standards

I hope you will agree there are some fantastic opportunities here that you can benefit from as a member of our industry Association – because we count on your support for each of these initiatives.

Please make the most of them.

FROM ATLANTA TO ROTTERDAM, A DEMAND FOR FREIGHT CRIME INTELLIGENCE & SOLUTIONS

I'm travelling a lot in September, and I expect to meet a lot of TAPA members along the way, and, hopefully encourage some new ones as I engage with large audiences from the security and insurance sectors.

I'll be presenting in Atlanta at *Global Security Exchange (GSX 2026)*, which runs from 14-16 September, and expects to attract over 20,000 delegates from more than 100 countries. Then, it's back to Europe, to address the *International Union of Marine Insurance (IUMI) 2026 Annual Conference* in Rotterdam, the world's largest marine insurance event on 22 September.

At both events, I'll be talking about freight crime trends, sharing data, and explaining how our industry Association and its members use this intelligence to make supply chains more secure, underpinned, of course, by the TAPA Standards. Are you attending GSX 2026 or IUMI? If you are, **I hope to see you there.**



FREE TRIAL CLOSES SOON...

The clock is ticking if you want to take advantage of the new *Certified Carrier Exchange*, developed by Trans.eu Group, based on TAPA Standards & Intelligence, and only featuring transport capacity from TAPA TSR Level 1 & 2 certified operators. If you've ever wanted a secure platform to source transportation for your high value loads, this is it. But the free trial finishes at the end of September. **Use the QR code on page 17 to sign up...**



A REMINDER TO REGISTER

We have events coming up in Portugal, Spain, and the United Kingdom, all with local language presentations and panel discussions – and all welcoming great speakers and panellists. If you have supply chain operations in these countries, please register now to support our preparations. These events are to help you understand freight crime risks in these countries and to build your supply chain resilience. **Please support us...**

REGISTER



SHOW YOUR DRIVERS YOU WANT TO PROTECT THEM

You may have seen our post announcing TAPA EMEA as one of the sponsors of a new initiative in the UK - *Driver Health Week*, which is from 1-6 September 2026.

We're in good company, supporting this initiative alongside National Highways, the Road Haulage Association, Logistics UK, Loughborough University, the Society of Occupational Medicine, and D4Group to promote healthy lifestyles for drivers as part of a new annual campaign aiming to support drivers and transport operators.

Professional drivers are vital to resilient supply chains and with much-publicised and longstanding driver shortages across

Europe and beyond, we have a responsibility to show our existing driver community how much we value them and want to ensure their health and wellbeing, and safety and security. This is also an important signal to others considering a professional driving career.

TAPA EMEA's UK Regional Lead, Harry Hughes, will be joining in the flagship event of *Driver Health Week - Driver Health Day* - on 4 September, which is going to bring together leaders from government, industry, healthcare, and academia to discuss the health and wellbeing of professional drivers, including speakers from Tesco, GXO Logistics, Evri and Whistl.

VISIT DRIVER HEALTH WEEK WEBSITE...

I also want to take this opportunity to remind you that, as a TAPA EMEA member, you are entitled to x50 free TAPA *Driver Security Awareness Training* courses – yet another opportunity to show your own driver pools that you are there to support them.

VISIT TAPA DRIVER SECURITY TRAINING WEBPAGE



TAPA EMEA'S FAMILY IS GROWING...

welcome

Introducing the latest companies to join us in our Europe, Middle East & Africa region...



17

COMPANIES & ORGANISATIONS



12

COUNTRIES

COMPANY	MEMBERSHIP TYPE	COUNTRY	WEBSITE
Circle UK Group Ltd	Security Service Provider	United Kingdom	VISIT WEBSITE >
CON.AP. Trasporti SRL	Country Full	Italy	VISIT WEBSITE >
De Rosa Trasport SRL	Full	Italy	VISIT WEBSITE >
Dea By E.S. Srl	Full	Italy	VISIT WEBSITE >
FCD Express Ltd	Full	Bulgaria	VISIT WEBSITE >
Grzebinoga Intertrans Transport i sp. z o.o.	Country Full	Poland	VISIT WEBSITE >
Hillcrest Advisory Group LLC	Consultancy	United States	VISIT WEBSITE >
In time express s.r.o.	Country Full	Slovakia	VISIT WEBSITE >
Kloiber GmbH	Parking Place Operator	Germany	VISIT WEBSITE >
Medical Logistic s.r.o.	Full	Slovakia	VISIT WEBSITE >
New Cargo Ltd GS Papanastasiou	Full	Greece	VISIT WEBSITE >
Pro Mile Ltd	Full	United Kingdom	VISIT WEBSITE >
Redington Gulf FZE	Country Full	United Arab Emirates	VISIT WEBSITE >
RFS Express SRL	Full	Belgium	VISIT WEBSITE >
Rolling Cars' 95 Kft.	Full	Hungary	VISIT WEBSITE >
Rozoti Prodcom SRL	Full	Romania	VISIT WEBSITE >
Secland Group Ltd	Parking Place Operator	United Kingdom	VISIT WEBSITE >

TO SEE ALL OUR 2026 MEMBERSHIP CATEGORIES, BENEFITS & COSTS

[CLICK HERE >](#)

FIGHTING FREIGHT FRAUD



The fraud patterns hitting supply chains today are not new. Banking and fintech lived through exactly those and spent a decade paying for it.

Fintech learned the hard way. Will logistics learn the lesson?

Freight fraud is one of the hottest topics of conversation and biggest concerns in the world of logistics. Already costing businesses hundreds of thousands or millions of euros in losses from a single criminal attack, it is accelerating at pace due to the focus of increasingly sophisticated organised crime groups and the ease and speed with which they are accessing and applying new technologies and AI tools to give their operations sufficient legitimacy and time to take control of high-value loads.

It's a phenomenon Karlheinz Toni first identified over a decade ago. Just not in logistics.

A serial entrepreneur, with more than 20 years of leadership experience across technology, finance, and private-equity-backed businesses, he previously led a Dutch online financing platform verifying six million identities on a yearly basis, both consumers and businesses, after regulators tightened the standards that the platform's original onboarding process had been built around. Not because the original checks were negligent. Because the bar moved, the threat evolved, and the identities that



had passed onboarding cleanly a year earlier could no longer be trusted to the new standard. He later focused on optimising KYB (Know Your Business) and KYC (Know Your Customer) processes, addressing the cost and complexity of fragmented business verification.

Now, as CEO and founder of TrustedCarrier, he applies this banking-grade approach to logistics, building a trusted digital identity infrastructure that enables carriers to verify their identity, credentials and compliance once, and share that trust across the European freight ecosystem.

So, what can logistics learn from the financial sector? In this special report, Karlheinz Toni shares his experience and the lessons that are now helping to secure supply chains across the globe...



The industry took years to learn how to identify who's on the other side of the screen and took way longer to build proper defences.

Logistics is where fintech was in 2012

The fraud patterns hitting supply chains today are not new. Banking and fintech lived through exactly those and spent a decade paying for it. Logistics is at the beginning of that same journey, but it doesn't have to repeat every mistake.

Twelve years ago, a wave of identity-based fraud was quietly dismantling trust in European financial services. It didn't look dramatic. There were no bank robberies. Instead, criminals were opening accounts with forged documents, impersonating existing customers, buying dormant legal entities and using their clean history to pass compliance checks.

Onboarding processes built for a slower, more analogue world were being gamed systematically by people who had studied them carefully.

The industry took years to learn how to identify who's on the other side of the screen and took way longer to build proper defences. It took even longer to get regulation to force security measures. The losses in between were enormous.

If we look at what is happening with company and personal identities in cargo and logistics, we can identify the same patterns.



The attacks are the same. The sector is different.

Phantom carrier fraud works by exploiting the gap between what a carrier appears to be and what it actually is. A criminal group presents a transport company - real documents, valid licence, registered address, possibly even positive platform ratings, and uses that identity to collect a load that it then disappears with. The cargo is gone before anyone realises the company collecting it wasn't who it claimed to be.

- **Synthetic identity fraud.** In fintech, this involves assembling an identity from a mix of real and fabricated elements, like a real registration number, a fabricated director, a genuine address, that passes automated onboarding checks and then builds a credible transaction history before the fraud occurs.



The three core techniques map directly onto the fraud patterns that fintech spent years learning to name and counter:

- **Account takeover.** In banking, this means a fraudster gains control of a legitimate customer's account and uses it to authorise transactions. In a Düsseldorf case decided in May 2026 (Landgericht Düsseldorf, reported by Trans.INFO), a criminal group accessed not a banking account, but a freight exchange platform account using the identity of a genuine, reputable forwarding company based in Bremen.

The mechanism was a single character: the real company's .de domain replaced with .com. From behind that cover, the group accepted transport orders and collected cargo. Total losses exceeded **€800,000**.

A BBC investigation broadcast in November 2025 found organised criminal networks in the UK doing exactly the same in logistics: acquiring legitimate haulage companies,



'None of these are new ideas. They are adaptations of tested attack patterns to a sector where the identity verification infrastructure is roughly where banking was before regulators forced it to modernise.'

sometimes using the identity of a deceased person, operating them as genuine subcontractors for long enough to establish credibility, then using that credibility to be assigned high-value loads. The official paperwork was real. The company history was real. The intent was not.

This subcontracting attack vector is now recognised at industry level. TAPA EMEA has just published its new *Subcontracting Guidance Document* because it understands the weakest link in a transport chain is rarely the contracted carrier. It is the second or third company down the chain that nobody verified. The guidance gives shippers and logistics providers a structured way to answer a question the BBC investigation showed that too few were asking: who is actually driving the load?

- **Urgency engineering.** Authorised Push Payment fraud, one of the most costly fraud categories in UK banking, works by creating artificial time pressure that prevents the target from pausing to verify and proceed to an action.

The logistics equivalent is embedded in the phantom carrier approach: urgent loads attract fraudulent carriers because urgency compresses the time available for verification, and because legitimate-sounding operational reasons for last-minute changes ("the original driver is sick, here are the new details") are harder to question when a shipment needs to move now.

None of these are new ideas. They are adaptations of tested attack patterns to a sector where the identity verification infrastructure is roughly where banking was before regulators forced it to modernise

What made fintech vulnerable then is what makes logistics vulnerable now

The fintech industry did not become a fraud target because it was careless. It became a target because three specific conditions converged at the same moment: a new product category moved fully online, identity documents that were faked or stolen, but looked real enough for online checks were perceived as real, and the fraud only surfaced when someone tried to collect on a debt that was never going to be repaid.

The product was short-term and small-ticket lending. Regulatory frameworks hadn't caught up yet, so lenders could issue loans entirely online, with no physical identity verification, no face-to-face check,

The financial services response to identity fraud went through roughly three phases, and the first two were expensive mistakes.



and no requirement to verify the applicant's identity against a government register rather than trusting the documents the applicant submitted themselves. That last detail is where everything broke. The documents weren't fake. They were genuine, stolen documents. Run them against official databases and they checked out, because they were the real thing attached to the wrong person. The fraud didn't announce itself until the loan went into default, a recovery team tried to reach the borrower at their registered address and phone number, and found someone who had no idea a loan existed in their name.

Logistics is running the same playbook in a different sector, at a higher ticket size, and with faster timelines. Freight management has moved online. Orders are placed on digital exchanges, documents are submitted by email or through platform portals, and the whole process from carrier approach to loading confirmation can happen in under an hour without anyone picking up a phone.

The identity documents submitted by a phantom carrier are not always forgeries in the crude sense. They belong to a real company. The transport licence is valid. The commercial register entry exists. The insurance certificate checks out. The fraud only surfaces when the consignee calls to ask where the load is or if an actual liveness check is done. The real carrier might say it never accepted the job, and someone finally dials the number on file and discovers it doesn't reach the company it was supposed to.

The root condition is identical in both cases: verification happened against the

document, not against an independent source. In fintech, it took regulatory pressure and years of losses to fix that. In logistics, the losses are already there.

€8.2b

Annual losses in Europe due to cargo theft

Source: European Parliament study

The German Insurance Association (GDV) tracked 88 confirmed phantom carrier cases in Germany alone in the first seven months of 2025, as many as in the entire previous year, with a full truckload disappearing every three days. UK freight theft losses rose from approximately £68 million in 2023 to £111 million in 2024, according to the TT Club and BSI Consulting, *Freight Crime Report 2026*.

These are not the numbers of a problem in its infancy. They are the numbers of a problem that has found its method and is scaling it.

Industry-level data points the same way. The TAPA Intelligence System (TIS), which collates cargo crime reports daily across the region, recorded more than 9,200 incidents in 78 countries in the first half of 2026, with a reported theft value above **€250 million** and losses averaging **€1.4 million** every 24 hours.

Even these figures understate the problem: over an 18-month period, fewer than 8% of the 58,661 incidents reported to TAPA EMEA included any financial data, according to the Association. In February, TAPA EMEA and IUMI, the International Union of Marine Insurance, whose members underwrite the majority of global cargo risk, issued a joint warning on fake carrier fraud.

Security associations and insurers rarely publish the same alarm at the same time.

What fintech got wrong first

The financial services response to identity fraud went through roughly three phases, and the first two were expensive mistakes.

- **The first instinct was to add friction at onboarding:** more documents, longer processes, more manual review. This slowed legitimate customers without stopping sophisticated fraudsters, who had better documents than most honest applicants.
- **The second instinct was to treat each attack as an isolated incident rather than a pattern.** A bank that suffered account takeover through a look-alike domain warning its own customers was useful. The same information not reaching competing banks or insurance carriers was not. Fraud networks, by contrast, shared intelligence and refined their methods continuously.
- **The third phase, which actually worked, was systemic:** standardised electronic identity verification against authoritative sources rather than submitted copies; continuous monitoring rather than point-in-time onboarding checks; risk-tiered verification where the depth of checks scales with the size and novelty of the transaction; and shared intelligence infrastructure so that a fraudulent identity flagged at one institution doesn't simply move to the next.

40% YoY

Rise of biometric fraud attempts

Source: Entrust 2026 Identity Fraud Report

'None of this requires waiting for regulation. The tools exist. The data sources exist. The question is whether the industry decides that carrier identity is a risk management problem, the way banks eventually decided that customer identity was a risk management problem, or continues to treat it as an administrative checkbox.'

The Entrust 2026 Identity Fraud Report finds that deepfake technology is now involved in approximately 20% of biometric fraud attempts in financial services, with AI-driven injection attacks rising 40% year-over-year, and notes that the tooling behind these attacks is increasingly available and affordable.

The TT Club and BSI Consulting's 2026 Freight Crime Report documents criminals already deploying AI-generated credentials and deepfake identities in logistics. The technological escalation that took a decade to arrive in fintech is arriving in logistics faster, because the tools are already built.

The lesson is not "Do what banks did" but to learn from them

It would be a mistake to conclude that logistics simply needs to copy the fintech compliance playbook.

The operational context is different, the regulatory environment is different, and some of what fintech built was driven by regulatory mandates that don't yet exist in transport, though eIDAS 2 (Regulation (EU) 2024/1183), which explicitly names transport as a sector where digital identity wallets must be accepted by December 2027, is closing that gap.

The transferable lesson is narrower and more specific: the unit of trust in logistics is the carrier identity, and that identity is currently verified the way a bank customer was verified in 2008 by looking at the document the counterpart hands you, rather than checking it against an independent authoritative source.

The three principles fintech eventually converged on apply directly.

1. Onboarding verification needs to run against primary sources

... like commercial register, VAT ID system, registered domain, transport licence database and not against submitted PDFs.

2. Carrier status needs ongoing monitoring

... not a one-time check at onboarding,

because a company that was legitimate when it registered on a platform may have been acquired by a criminal network since.

3. Verification intensity needs to scale with risk

... a routine load to a long-standing carrier and a high-value first assignment to a recently registered company are not the same transaction and should not be treated identically.

Parts of the industry are already moving in this direction. In June 2026, at its *Annual Conference* in Oberhausen, TAPA EMEA and Trans.eu Group, the European freight tech and fintech company whose digital ecosystem connects more than 44,000 carriers, freight forwarders and shippers, launched the *Certified Carrier Exchange*.

It is the first freight exchange built entirely on verified security certification: only carriers holding a valid TAPA TSR Level 1 or 2 certification can offer capacity, and their status is not self-declared but verified automatically, in real-time, against TAPA's own database.

It is a working demonstration of the third-phase principle: "trust anchored in an independent authoritative source, continuously validated, not a PDF submitted once at registration."

None of this requires waiting for regulation. The tools exist. The data sources exist. The question is whether the industry decides that carrier identity is a risk management problem, the way banks eventually decided that customer identity was a risk management problem, or continues to treat it as an administrative checkbox

Where this leads to without action

Fintech's decade of friction was expensive in ways that went beyond direct fraud losses. Insurance premiums rose. Regulators imposed requirements that cost far more to implement under pressure than they would have cost to build proactively. High-profile fraud cases changed customer behaviour in ways that took years to reverse. The industry

didn't choose that path. It just didn't choose the alternative fast enough.

The trajectory in logistics is not inevitable, but it is visible. Cargo insurance premiums for high-risk categories are already moving. Underwriters are starting to ask questions about carrier verification processes that most shippers and LSPs are not used to answering. The Düsseldorf conviction made headlines because it made the mechanism legible to people outside the industry. The BBC investigation did the same. Neither story surprised anyone who had been watching the data. Both stories surprised almost everyone else.

That gap between those paying attention and those who aren't is exactly where organised crime operates.

The networks running phantom carrier schemes today did not start from scratch. They inherited a toolset that fraud networks in financial services spent a decade refining: AI-generated documents, acquired legal entities with clean histories, coordinated multi-vehicle operations timed for peak periods, and social engineering scripts tested across thousands of attempts. They got to this level of sophistication faster than fintech fraudsters did, because the tools were already built. All they had to do was redirect them.

What doesn't transfer from fintech is the timeline. Logistics doesn't get a decade to figure this out. The acceleration is already baked in. Thanks to AI.

Running that exercise at scale, in real time, on a live platform with active customers, is a different problem entirely from building verification correctly from the start. That experience is a direct input into how Trusted Carrier was designed.

Verification infrastructure built to evolve, not to be replaced

The question isn't whether phantom carrier fraud becomes a systemic problem. It already is one. The question is whether the industry builds the verification infrastructure before regulators mandate it under crisis conditions, before insurers price out the high-risk segments, and before a handful of high-profile cases shift shipper behaviour in ways that take years to recover from.

Fintech learned that lesson the hard way, at a cost that ran into billions and took the better part of a decade to work through. The shortcut exists. The infrastructure model is proven. The only thing missing is the decision to build it now rather than after the damage makes it unavoidable.

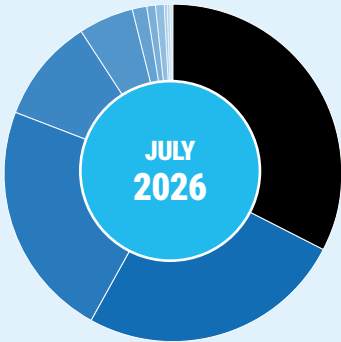
EUROPE, MIDDLE EAST & AFRICA REGION

CARGO CRIME MONITOR



€22,488,904

Total loss for the 238 or 22% of crimes stating a value



JULY 2026

LOCATION TYPE

Unknown	352	32.75%
Retail Store	275	25.51%
Origin Facility	245	22.73%
En Route	108	10.02%
Services 3rd Party Facility	57	5.29%
Unclassified Parking	15	1.39%
Maritime Transportation Facility	10	0.93%
Railway Operation Facility	6	0.56%
Aviation Transportation Facility	5	0.46%
Destination Facility	3	0.28%
Road Transportation Facility	1	0.09%



€492,351

Average loss for the 40 recorded cargo thefts with a value of €100,000 or more reported to the TAPA EMEA Intelligence System (TIS) in July 2026

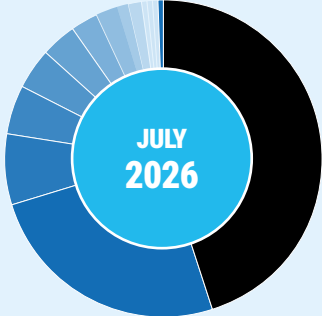
17

Crimes in EMEA recording a loss value of between €50,000 & €100,000, totalling €1,209,397

21

Number of TAPA TIS product categories recording losses in July 2026





JULY 2026

INCIDENT CATEGORY

Theft from Facility	487	45.18%
Theft from Vehicle	272	25.23%
Robbery	79	7.33%
Theft of Vehicle	54	5.01%
Counterfeit	44	4.08%
Hijacking	40	3.71%
Theft	28	2.69%
Truck Theft	23	2.13%
Theft of Trailer	14	1.30%
Fraud	13	1.21%
Theft from Container	7	0.65%
Theft of Container	6	0.56%
Clandestine	6	0.56%
Theft from Trailer	4	0.37%





11.7%

Or 127 of the reported incidents stated an M.O. of Violent or Threat with Violence



1,077

Number of new cargo crimes reported to the TIS database in July 2026

€60,602

Average loss for all cargo crimes reported with a value



€3,000,000

BIGGEST REPORTED LOSS IN JULY 2026: A Theft from Facility of miscellaneous goods in Békéscsaba, Hungary, on 22 July with an Internal M.O.

CARGO THEFT BY COUNTRY


S3

 Number of countries in
EMEA reporting incidents

JULY 2026

TOP 5

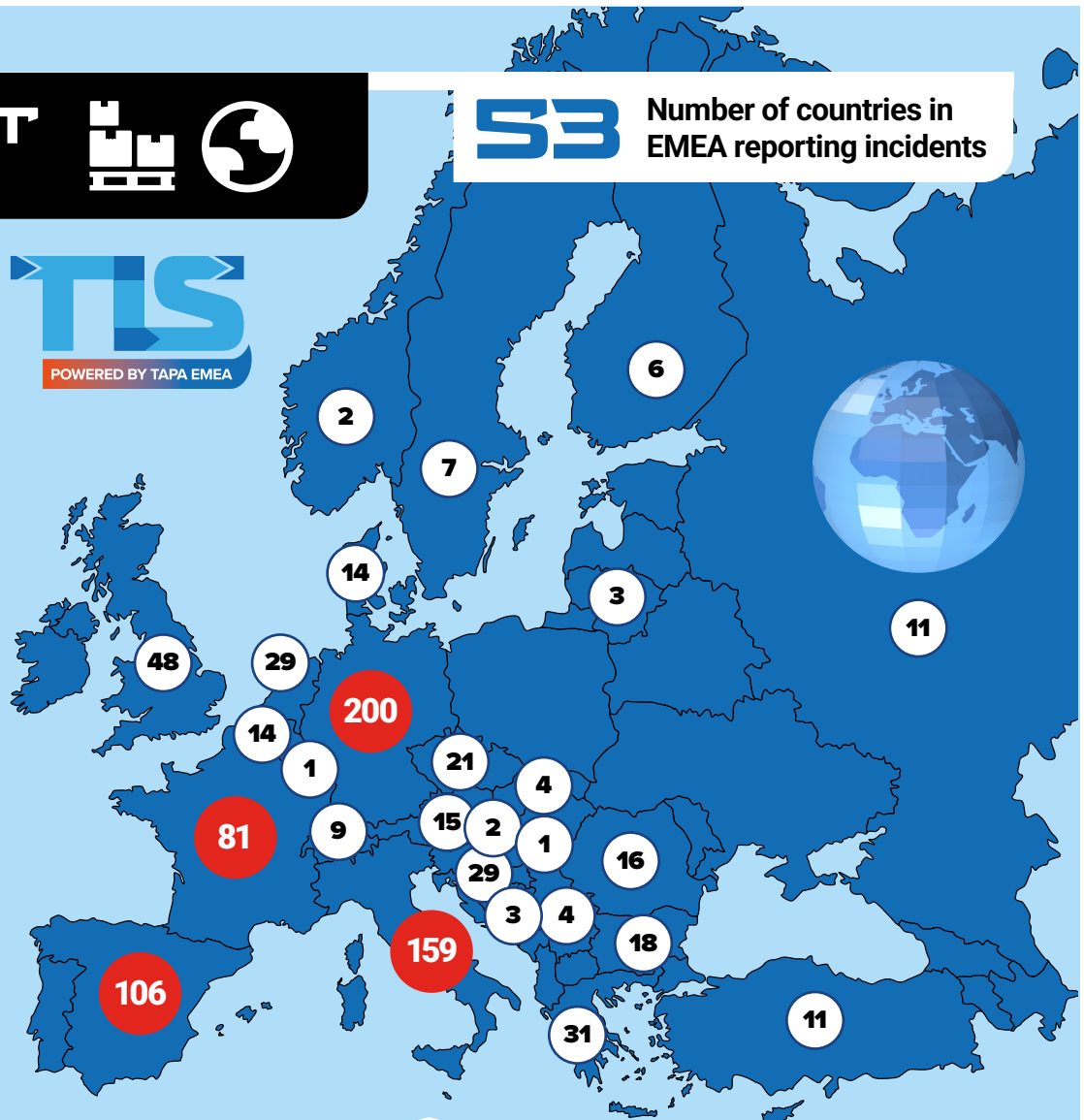
Germany	200
Italy	159
South Africa	131
Spain	106
France	81

Rest of EMEA

Morocco	4
Serbia	4
Slovakia	4
Yemen	4
Bosnia and Herzegovina	3
Algeria	3
Lithuania	3
Norway	2
Slovenia	2
Libya	2
Iraq	2
Eswatini	2
Ghana	2
Mozambique	2
Mauritius	2
Syrian Arab Republic	1
Kenya	1
United Arab Emirates	1
Ethiopia	1
Hungary	1
Somalia	1
Palestine	1
Luxembourg	1
Cameroon	1
Saudi Arabia	1
Malawi	1
Namibia	1
Oman	1

Rest of EMEA

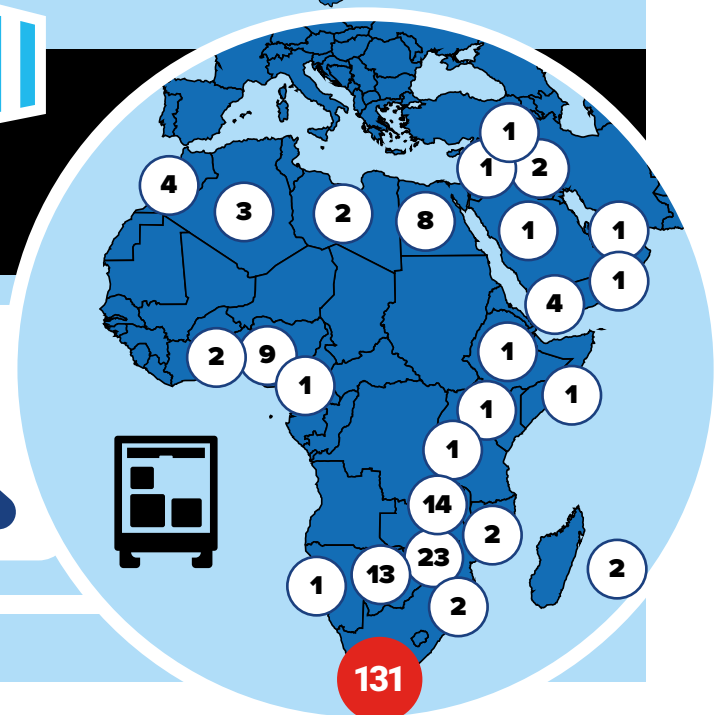
United Kingdom	48
Greece	31
Netherlands	29
Croatia	29
Zimbabwe	23
Czechia	21
Bulgaria	18
Romania	16
Austria	15
Denmark	14
Belgium	14
Zambia	14
Botswana	13
Turkey	11
Russian Federation	11
Switzerland	9
Nigeria	9
Egypt	8
Sweden	7
Finland	6

TOTAL RECORDED INCIDENTS: 1,077

DAILY LOSS FOR INCIDENTS REPORTED IN JULY 2026

€725,448

**MODUS OPERANDI
USED IN
LATEST
CARGO
THEFTS:**

Intrusion	705	65.40%
Unknown	158	14.75%
Violent & Threat with Violence	127	11.78%
Deception Other	59	5.47%
Internal	24	2.23%
Deceptive Pick Up	3	0.28%
Theft from Moving Vehicle	1	0.09%





TAPA EMEA and ADSP in action: Protect the Supply Chain

LISBON – 30 SEPTEMBER 2026 – REGISTER NOW...

TAPA EMEA and ADSP - the Association of Security Directors of Portugal, the leading national association of security professionals, invite you to join us in Lisbon on 30 September as we bring our members and industry stakeholders together to discuss protecting supply chains against criminal attacks as freight crime escalates across Europe.



In the last 18 months in the Europe, Middle East & Africa (EMEA) region, the TAPA Intelligence System (TIS) has recorded:

- **>58,000** freight theft incidents
- **>€1 billion** in losses from supply chain thefts
- An average loss of **€1,086,285** for major crimes (**€100K+**)
- Equal to **€1,870,271** of goods stolen from transport and facilities every 24 hours.

And, today, virtually all types of products are a target for organised crime groups and others, including:

- | | |
|-------------------------------|------------------------------------|
| • Metal | • Tobacco |
| • Cash | • Agricultural Machinery |
| • Tools & Building Materials | • Bicycles |
| • Food & Drink | • Furniture & Household Appliances |
| • Jewellery & Precious Metals | • Tyres |
| • Electronics | • Sports & Fitness Equipment |
| • Clothing & Footwear | • Computers & Laptops |
| • Cosmetics & Hygiene | • Toys & Games |
| • Phones | • Pharmaceuticals |
| • Auto Parts | |

What more can manufacturers and logistics service providers do to protect their supply chain operations in Portugal from attacks by organised crime groups and other offenders?

On **30 September 2026 in Lisbon**, TAPA EMEA and ADSP will bring together industry leaders and law enforcement agency professionals to look at the causes of freight crime in Portugal and Europe as well as police work to disrupt crime groups. The event will also present proven security solutions already protecting supply chains across Europe, and the cargo crime incident intelligence driving this industry response.

Our **Portuguese language** conference is free to join but delegate places are limited, and only available on a first come, first served basis.

Register now... and join us in Lisbon to learn more about protecting your supply chain and preventing the financial and reputational impact of a criminal attack.

REGISTER NOW



NO SUMMER BREAK FOR CRIME GROUPS TARGETING SUPPLY CHAINS, WITH >€22.4M OF LOSSES REPORTED IN JULY ACROSS 53 COUNTRIES

There was no summer recess for criminals targeting supply chains in Europe, the Middle East & Africa in July, with the TAPA Intelligence System (TIS) receiving reports of another 1,077 freight crimes in 53 countries.

Only 238 or 22% of the incidents reported to TAPA EMEA in July shared their financial loss, but those that did contributed to a combined loss of >€22.4 million. This figure alone meant that over the 31 days of the month, the value of reported cargo crimes averaged €725,448 every 24 hours.

Major thefts (€100K+) targeting goods in facilities, carried onboard trucks as well as other modes of transport, produced an average loss of €492,351 for the 40 highest-value crimes added to the TIS database.

The top five countries for recorded cargo thefts in July accounted for 62.8% of all incidents:

- **Germany** – 200 freight thefts, 18.5% of the July total
- **Italy** – 159 or 14.7%
- **South Africa** – 131 or 12.1%
- **Spain** – 106 or 9.8%
- **France** – 81 or 7.5%



Another 15 countries saw double-digit incidents rates: United Kingdom (48), Greece (31), Croatia (29), Netherlands (29), Zimbabwe (23), Czechia (21), Bulgaria (18), Romania (16), Austria (15), Belgium (14), Denmark (14), Zambia (14), Botswana (13), Russia (11), and Turkey (11).

Of the 1,077 crimes reported to TIS during the month of July, 692 occurred during the month. The other incidents took place earlier. The 692 crimes represented €10.3m (based on 147 or 21.2% sharing their loss value) of the €22.4m referenced earlier.



In total, 28 major thefts with losses of €100K+ came from incidents that took place during the month. These included two seven-figure losses:

€3,000,000

The biggest reported loss in July occurred on 22 July. Employees fraudulently stole a shipment of miscellaneous goods worth €3m from their company's premises in Békéscsaba in southeast Hungary.

€1,000,000

Five offenders carried out a ram-raid at a recently-opened jewellery Retail Store in Pescara, Italy, on 10 July at around 04:20am, using a stolen vehicle to smash through the entrance. The gang stole jewellery and other valuables before escaping in a large vehicle.



Other major freight thefts reported to TAPA EMEA in July also included:

€481,000

Spanish authorities arrested 10 members of an international crime group suspected of carrying out 11 cargo thefts from moving trucks across Spain.



The group used the highly dangerous "surfer method", using powerful cars to isolate



target trucks before an accomplice climbed from a specially modified vehicle onto the moving trailer, forced open the locks, and transferred goods while in motion. The largest theft reportedly involved €400,000 of tobacco products near Toledo. The suspects were arrested on 7 July following the theft of 16 televisions. Police also seized modified vehicles, specialist tools, communications equipment, and foreign license plates

€370,000

Greek Police dismantled an organised gang responsible for a series of jewellery store burglaries across Attica. The group allegedly used stolen vehicles and concealed their identities while targeting stores, forcing security shutters or smashing windows to steal high-value gold jewellery. Nine suspects were arrested on 4 July.

€330,000

Law enforcement officers made four arrests on 22 July of individuals suspected of stealing textiles and electronic devices from a company warehouse in Hoče, Slovenia, over an extended period.



Police believe two employees worked with two other suspects to systematically remove goods from the business. Searches in the Maribor and Lenart areas resulted in the recovery of a significant quantity of suspected stolen merchandise.



Spain suffers one of the highest rates of freight crime in Europe

TAPA EMEA REGIONAL CONFERENCE

Madrid – 21 October 2026

Over 2 years to the end of June 2026, the Transported Asset Protection Association (TAPA) recorded over 4,200 attacks on trucks, warehouses, and other types of facilities and modes of transport in Spain. The 13% of these cargo crimes reporting a loss value contributed to a total loss of goods in Spain of >€197 million.

Major losses (€100K+) of products in supply chain attacks in Spain averaged €1,336,836.

Today, virtually all types of goods are a target for criminals in storage and in-transit, including...

- Metal
- Cash
- Tools & Building Materials
- Food & Drink
- Jewellery & Precious Metals
- Electronics
- Clothing & Footwear
- Cosmetics & Hygiene
- Phones
- Auto Parts
- Tobacco
- Agricultural Machinery
- Bicycles
- Furniture & Household Appliances
- Tyres
- Sports & Fitness Equipment
- Computers & Laptops
- Toys & Games
- Pharmaceuticals

What more can manufacturers and logistics service providers do to protect their supply chain operations in Spain from attacks by organised crime groups and other offenders?

On **21 October 2026** in **Madrid**, TAPA will bring together industry leaders and law enforcement agency professionals to look at the causes of freight crime in Spain as well as police work to disrupt crime groups. The event will also present proven security solutions already protecting supply chains across Europe, and the cargo crime incident intelligence driving this industry response.

Our conference is **free to join** but delegate places are limited, and only available on a first come, first served basis.

We invite you to join us in Madrid to learn more about protecting your supply chain in Spain and preventing the financial and reputational impact of a criminal attack.

TAPA EMEA members can register **one** delegate free of charge under their membership benefits. Additional delegate places cost €250.00 per person. Please note TAPA EMEA's **No-Show Policy** will apply to this event. Details on conference website.



ALL PANELS & PRESENTATIONS IN SPANISH

REGISTER NOW



€200,000

Thieves also stole jewellery and gold bars from a jewellery store in Agrigento, Italy, on 8 July, after first breaking into an adjacent laundry premises and cutting a hole in the adjoining wall.

**€200,000**

Some **€200,000** of products were stolen from a coffee-roasting company in an industrial area in Italy after offenders entered the warehouse during the night to target high-value merchandise. The theft on 5 July was only discovered when the business reopened. Police are analysing CCTV footage and investigating whether the offenders are connected to a series of other recent thefts targeting businesses in the same industrial area.

€200,000

Six masked offenders stole jewellery and watches from a Retail Store in Mestre, Italy, in a raid lasting just four minutes on 17 July. The gang used a hydraulic spreader to open the reinforced entrance before emptying display cases and fleeing in waiting vehicles.

**€164,000**

In an undisclosed region of Romania on 7 July, a fake carrier sent a truck with false license plates to collect a large shipment of cosmetic goods, which later disappeared.

**€110,000**

A truck carrying 70,000 cans of drinks belonging to a company co-owned by a well-known Dutch YouTuber disappeared whilst en route in Germany on 16 July. Around 20,000 cans have since been traced after products matching the stolen batch were discovered at a market in Tilburg and on the Beverwijk black market.

**€103,284**

Bulgarian customs officers intercepted a Serbian-registered truck near Vidin, Bulgaria, on 2 July, carrying 626,600 cigarettes concealed inside specially constructed double panels. The Croatian driver had claimed the truck was empty while travelling from Serbia to Romania.

€100,000

Two offenders stole a semi-trailer loaded with alcoholic spirits in Rastatt, Germany, at



around midnight on 30 July. The suspects reportedly arrived in a white tractor unit and connected it to the trailer, which was left in an unsecured parking location.

The 13 cargo crimes in July recording loss values of between €50K-£100K included:

- **€91,000** - A series of businesses were targeted between Gallese and Civita Castellana in the Viterbo area of Italy, resulting in losses of trucks and other commercial vehicles from company premises. The incidents have raised concerns among local businesses about a potential organised crime group specialising in high-value vehicle thefts.
- **€90,000** - A truckload of 20 tonnes of Emmental cheese disappeared while being transported from a dairy in Bayreuth, Germany, to France on 14 July. The original freight company had subcontracted the delivery through an online freight exchange. The truck and driver that collected the cheese never arrived at the destination in France.
- **€80,000** - At least eight masked offenders raided a jewellery store in Petroupoli, Athens, Greece, shortly after 04:00am on 14 July. The gang arrived in two vehicles and, after failing to lift the security shutters, attached them to a vehicle with a strap and ripped them away. Four offenders then entered and emptied the store within minutes, reportedly using fire extinguishers to obscure evidence before escaping. The raid was captured on CCTV and police are investigating possible links to similar burglaries in the area.
- **€60,000** - At least four offenders targeted an opticians Retail Store in Rezzato, Italy, at around 01:30am on 21 July, stealing eyewear and other valuable products, and causing an additional **€10,000** in damage. The gang blocked access to the car park with pallets and bins before smashing through the security shutter and shop window.
- **€55,000** - On 22 July, six employees of an international freight transport company were detained in Romania on suspicion of stealing goods from cargo shipments they were responsible for transporting on international routes between March and June 2026. Police carried out seven searches in Prahova and Buzău,



recovering laptops, clothing, cosmetics, and electronics believed to be connected to the offences.

- **€50,000** - A professional gang targeted a car dealership in Brescia, Italy, on 10 July, stealing a high-performance vehicle worth more than **€50,000**. The offenders had allegedly visited the showroom days earlier posing as customers and stole the vehicle's keys before returning overnight, forcing entry, and then using another vehicle from the dealership as a battering ram to break through the exit gate.

TAPA EMEA members can see all the latest cargo crime incident intelligence in the TIS password-protected database.



STOLEN PRODUCTS	No.	%
TOP FIVE		
Miscellaneous	303	28.20%
Fuel Theft	144	13.36%
Cash	95	8.81%
Unspecified	76	7.05%
Metal	68	6.31%
TOP FIVE TOTAL	686	63.73%
Jewellery/Precious Metals	64	
Tools/Building Materials	53	
No Load (Theft of truck and/or trailer)	50	
Food & Drink	50	
Clothing & Footwear	35	
Cosmetics & Hygiene	34	
Tobacco	17	
Miscellaneous Electronics	16	
Bicycles/Two Wheelers	12	
Pharmaceuticals	11	
Phones	11	
Auto parts	10	
Tyres	9	
Furniture/Household Appliances	8	
Agricultural Materials	5	
Sports & Fitness Equipment	3	
Toys/Games	2	
Computers/Laptops	1	
OTHER PRODUCTS	391	36.27%

WHEN SECURITY RULES BLOCK ACCESS TO SECURE CAPACITY

Shippers restrict freight exchanges to protect their cargo. But when every exchange is treated the same way, those same rules can prevent freight forwarders from accessing the high-security capacity their customers need.

For companies transporting electronics, pharmaceuticals, high-tech products, automotive components, luxury goods, and other high-value or theft-sensitive cargo, carrier selection is about much more than finding an available truck. The performing carrier needs to be known. The security requirements need to be met. Subcontracting needs to remain controlled, and the transport operation needs to match the value and risk profile of the cargo.

It is therefore understandable that many shipper-forwarder agreements restrict or completely prohibit the use of freight exchanges — digital marketplaces where transport capacity is sourced from a broad, often unverified, pool of carriers. The intention is clear: prevent uncontrolled subcontracting, re-brokering, unknown carriers, and loss of visibility over who actually performs the transport.

But there is a growing problem with this approach. Many contracts treat every freight exchange as if it were the same — regardless of whether the carriers behind it are unverified, or TAPA TSR-certified and independently assessed.

The problem is not the lack of protection. It is the assumption that all freight exchanges are the same.

A contract clause is blocking your safest capacity.



The difference between a traditional freight exchange and the Certified Carrier Exchange

At one end of the spectrum are traditional freight exchanges, where the primary function is to connect supply and demand. A company may receive carrier contact information, but much of the responsibility for evaluating the carrier — and deciding whether it is suitable for the shipment — remains with the user.

The *Certified Carrier Exchange*, powered by TAPA EMEA Standards & Intelligence, adds another security layer.

It brings together a restricted community of carriers holding valid TAPA TSR 1 or TSR 2 certification. The value of the community lies not only in the fact that participating companies have been verified — it is also the security capability behind those companies.

TSR-certified carriers operate fleets and transport processes assessed against defined TAPA Trucking Security Requirements. These requirements address areas such as physical vehicle security,

locking, tracking and monitoring, security procedures, and incident response.

In other words, the difference is not simply who is allowed onto the platform. It is also the security standard the carrier is expected to operate to during the physical execution of the transport.

For a company transporting high-value goods, this changes the sourcing question.

It is no longer simply: **"Where can my forwarder find another truck?"**

It becomes: **"Where can my forwarder find additional capacity that meets the security expectations of this shipment?"**

That is a very different requirement.

High-value cargo needs more than available capacity

During normal operations, contracted carrier networks remain the preferred solution for most shippers. But transport demand does not always follow the plan.

When volumes increase, peak seasons put pressure on available capacity. A regular carrier becomes unavailable. An urgent



transport requirement appears. A difficult lane suddenly needs additional coverage.

At that point, the forwarder is expected to react.

For high-value cargo, however, simply finding another transport provider is not enough — the alternative carrier must also satisfy the required security conditions. This creates a potential contradiction in some shipper policies.

The forwarder may have access to a community of TSR-certified carriers capable of providing the required secure transport, but the shipper's contract may prevent the forwarder from using that sourcing channel because it falls under a broad definition of a "freight exchange."

The capacity exists. The security capability exists. But the contractual framework prevents access to it.

This can turn a security restriction into a business-continuity issue.

When a security rule creates another risk

The intention behind a no-freight-exchange clause is to reduce risk.

But different types of freight exchanges provide different levels of security. Putting them all in the same bucket can create another set of risks.

For high-value goods, the problem can become even more acute, because the pool of carriers capable of meeting stringent

security requirements is already more limited than the general transport market.

A blanket prohibition may therefore remove exactly the sourcing options that could help when secure capacity is hardest to find. The answer is not to weaken security requirements — it is to make the policy more precise.

From "no freight exchanges" to "approved secure sourcing"

Instead of asking whether freight exchanges should be allowed or prohibited, shippers could ask a more useful question:

Which sourcing environments meet our security requirements, and under what conditions should our nominated logistics providers be allowed to use them?

This creates the possibility of a more differentiated approach.

A shipper may continue to prohibit the use of traditional open freight exchanges while explicitly recognising the *Certified Carrier Exchange* as an approved sourcing channel under defined conditions. The principle is important: **Manage the security controls in a more precise way.**

The fleet matters

There is another reason why the distinction matters for high-value shippers. Much of today's discussion about digital freight sourcing concentrates on platform security and carrier verification. Both are essential. But the cargo is not ultimately protected

by the platform. It is protected during execution — by the carrier, the vehicle, the technology, and the security procedures surrounding the transport.

This is where the TSR 1 and TSR 2 carrier community becomes particularly relevant.

The security conversation therefore needs to move beyond *"Is the carrier verified?"* towards *"Does the carrier operate the fleet and processes required for secure transport?"*

For high-value goods, that is arguably the more important question. An available carrier is not necessarily a suitable capacity.

Secure capacity means having the right carrier, the right fleet, and the right security level available when the shipment requires it.

Secure capacity without losing control

Uncontrolled subcontracting, insufficient carrier verification, and loss of visibility remain real concerns, particularly for high-value and theft-sensitive goods. But a restricted community of TSR-certified carriers should not automatically be evaluated in the same way as a traditional open freight marketplace.

As demand for secure transport capacity grows, shippers need both control and flexibility. The opportunity, therefore, is not to move from restriction to unrestricted access.

It is to move from blanket prohibition to controlled permission.

A free trial of the *Certified Carrier Exchange* is available only until the end of September — a timely opportunity for shippers and their logistics partners to put this differentiated approach into practice. Start your free trial using the QR code below...

Standard freight exchange access

- ✓ Flexible carrier sourcing
- ✓ Platform-based verification
- ✓ Wide market access
- ✓ Suitable for everyday transport needs

Certified Carrier Exchange powered by TAPA EMEA Standards & Intelligence

- ✓ **Carriers audited** against strict TSR security requirements
- ✓ **Verified procedures** for parking, routes, and cargo protection
- ✓ **Reduced need** for manual security checks and onboarding
- ✓ **Dedicated environment** for high-value and sensitive cargo

Start your free trial

Free access ends September 30



FREIGHT CRIME IN THE UK: THE MOMENTUM IS THERE, BUT WE NEED TO MOVE FASTER

By Harry Hughes, UK Regional Lead, TAPA EMEA



When I took on the role of UK Regional Lead for TAPA EMEA, I already knew freight crime was a serious

issue. I run a transport business myself, so I understand the responsibility that comes with moving somebody else's goods and the pressure operators and drivers face every day.

What the role has given me is a much broader view of the problem.

I have now spoken with transport operators, manufacturers, logistics buyers, insurers, security specialists, police officers, government representatives, and other organisations that represent our industry. I have attended conferences, joined roundtables, visited businesses, and taken part in meetings covering secure parking, driver welfare, organised crime, fraud, and intelligence sharing.

There are some brilliant people working in this area and there is definitely momentum building in the UK to tackle freight thefts and target those responsible. My concern is the speed of the overall response. We are having the right conversations and getting the right people around the table. That is important, but we now need to turn more of those conversations into something practical that operators and drivers can actually use.

One thing has become very clear to me: no single organisation can tackle freight crime on its own. The police cannot solve it without information from the industry. Operators cannot manage the risk properly if customers do not understand how their requirements work in the real world. Drivers cannot park securely if there are not enough suitable places for them to stop.

We all have a part to play, and we need to get much better at joining those parts together.

Has the UK transport sector woken up to freight crime?

I think the sector is waking up to the threat, but I would not say we are completely there yet in terms of a coordinated response. Some companies understand freight crime extremely well. They have experienced security teams, proper risk assessments, good technology and clear procedures. They invest in vehicle security, secure facilities, driver training, route planning, monitoring, and secure parking.

They understand that security is not just a tracker on a vehicle or a lock on the back door. It is about people, processes, equipment, intelligence, and communication all working together.



'We are dealing with organised criminals who understand logistics. They know how transport businesses work and where the weaknesses are likely to be. Sometimes they know far more about a load than we would like them to know.'

But let's be honest: the level of understanding across the wider industry is still very mixed. Some businesses only realise how exposed they are after they suffer a major loss, narrowly avoid one, or are challenged by a customer or insurer over their supply chain security.

Others know freight crime is happening but still think of it mainly as somebody cutting a tarpaulin curtain or breaking into the back of an unattended vehicle.

That is part of the problem, but the threat goes much further than that.

We are dealing with organised criminals who understand logistics. They know how transport businesses work and where the weaknesses are likely to be. They can target specific goods, produce false paperwork, impersonate legitimate carriers, interfere with subcontracting arrangements, and exploit information available online.

Sometimes they know far more about a load than we would like them to know.

The organised crime groups behind these offences often have highly sophisticated supply chains of their own. In some cases, they can move stolen products across borders quicker than legitimate businesses can.

They do not have to follow drivers' hours directives, customs processes, security procedures, or any of the other rules and regulations that legitimate operators have to follow. By the time an incident has been reported and the information has reached the right people, the goods may already have passed through several countries.

That is what we are up against.

We also have to recognise the commercial and operational pressure on transport companies. Margins are tight, delivery windows are demanding, and suitable secure parking is still far too limited. A customer can specify strict security conditions, but those conditions need to work in the real world. They also need to be considered when the service is planned and priced.

It is too easy to write a long list of requirements into a contract and place all the responsibility onto the haulier and, ultimately, the driver. If a driver reaches the end of their permitted hours and the nearest suitable parking location is full, what are they realistically expected to do? If the route and delivery window have been planned

without considering where that driver can stop, the problem has already been created before the vehicle leaves the depot.

So, yes, I think the UK is waking up. There is far more discussion about freight crime and supply chain security than there was previously - but talking about the problem does not protect the load. Awareness has to lead to better planning, proper investment, and genuine cooperation.

Getting companies interested in the TAPA Standards

One of TAPA EMEA's biggest strengths is that we don't just talk about security and gather freight crime intelligence. We have practical Standards that businesses can use to make their supply chain operations more secure.

TAPA's Facility Security Requirements (FSR), Trucking Security Requirements (TSR) and Parking Security Requirements (PSR) give companies clear frameworks for identifying risks and improving their operations. SME operators can also gain a lot of benefits from the Association's latest Cyber Security Standard.

I am definitely seeing more interest from UK companies, including businesses that are not currently certified to a TAPA Standard. They want to understand what certification involves, which level would be suitable for them, and whether it will help with enhancing their reputations with customers and drive future business opportunities.

That is encouraging, but we still have a lot of work to do. If somebody is new to TAPA,





the Standards can initially look like another audit, another cost, and another layer of administration. I understand that response because, as I said, I run a transport business. I know what it is like when somebody sends you another set of requirements and expects you to absorb all the cost and work involved.

The difference comes when Standards are treated as practical operational tools rather than another compliance exercise. And it comes from when they help a company identify gaps, set clear expectations, and demonstrate that its security arrangements have been independently assessed and certified. They also give customers and transport providers a common language.

Instead of a customer simply asking for a "secure vehicle" or telling an operator to use "secure parking," both sides can have a proper conversation about what that actually means. TAPA Standards are not just certificates to display on a wall.



'The difference comes when Standards are treated as practical operational tools rather than another compliance exercise. They also give customers and transport providers a common language.'

Their value comes from the decisions they influence every day: how a facility controls access, where a driver stops, how a vehicle is monitored, what happens when an alarm is triggered, and how quickly an incident is escalated.

Secure parking is our biggest challenge

For me, the lack of secure parking is the biggest challenge to supply chain security and the area that needs the most attention, particularly in the UK.

I have been having some excellent meetings through the SCRIP (Supply Chain Risk Intelligence Partnership) parking subcommittee. Markus Prinz and Pana Laimos from TAPA EMEA have also joined in these discussions, and there is a clear drive from everyone involved to improve the quality and availability of secure freight parking across the UK.

But again, we would like to see this move faster.

We cannot keep telling drivers to park securely when we do not provide enough safe and suitable places for them to stop. It is very easy to put "secure parking must be used" into an operating procedure. Delivering that instruction on the road at the end of a driver's working day is something very different.

A large proportion of reported UK freight crime happens at motorway service areas, and that is a problem in itself. These sites are heavily used and often full every night. At the same time, many motorway sites are going to find it extremely difficult to achieve TAPA's Parking Security Requirements without major investment and a genuine long-term commitment to improving security.

This is not something that can be fixed by putting up another camera or adding a small section of fencing. Proper security needs an overall plan. That includes

the perimeter, entry and exit controls, surveillance, lighting, monitoring, incident response, and the safety and welfare of the drivers using the site.

We also need to be much clearer about the word "secure."

A parking location should not be described as secure just because it has a fence, a camera or somebody sitting near the entrance. Operators and drivers need to know what level of protection is actually in place and what will happen if there is an incident. One development that gives me some optimism is the number of new multi-fuel sites being planned to support the decarbonisation of road transport. Many of these sites are being designed and built from the ground up – and this gives developers the chance to include proper security and driver welfare from day one instead of trying to add it later.



TAPA EMEA
Transport Asset Protection Association



'Police need more than a report saying that goods have been stolen. Useful information can include exact times and locations, vehicle and trailer details, tracking data, CCTV, telephone numbers, email addresses, false paperwork, and descriptions of suspicious people or vehicles.'

Several sites are already considering TAPA PSR or other recognised parking standards as part of their plans. If these new sites can provide good security, decent facilities, and reliable parking spaces, they could create real competition, and greater supply chain resilience. Existing providers may then have to improve security response because operators and drivers will have a better choice. That could be the start of a much-needed wave of positive change.

Personally, I would also like to see the industry develop a specific security standard or rating system for motorway service areas, but I am also realistic. Every motorway service area is not going to achieve TAPA PSR overnight. Some may struggle to achieve it at all without major changes.

However, we should still be able to assess these locations consistently and give transport operators and drivers a clear view of which sites offer the highest security. That rating could be linked to reported freight crime data for the individual motorway service area. An operator planning a route could then see what facilities and security measures are available, as well as the level of reported crime at that location.

At least that would allow potential users to make a better-informed decision.

It would also recognise the motorway service areas that are investing and making meaningful improvements, while showing clearly where more work is needed.

TAPA's Parking Security Requirements already provide an internationally recognised framework. The important thing is using that framework to improve real decisions about where vehicles stop, what protection drivers can expect, and how quickly an incident will be identified and escalated.

Industry and law enforcement need each other

My discussions with NaVCIS, the National Vehicle Crime Intelligence Service (NaVCIS) Opal, the UK's National Intelligence Unit for Serious and Organised Acquisitive Crime, as well as other police officers, have shown me how important the relationship between industry and law enforcement really is. NaVCIS has developed considerable specialist knowledge around freight and vehicle crime in the United Kingdom, while OPAL's nationwide work on tackling serious organised acquisitive crime, including organised supply chain theft, gives us another real opportunity to improve coordination.

This matters because organised criminals do not care about police force boundaries.

A vehicle may be loaded in one region, targeted in another, and the goods moved somewhere completely different. The same group may be committing offences across several police areas or several countries. If each incident is looked at on its own, the connection may never be seen. Bring the information together and a very different picture may emerge. That is why the quality and speed of information from industry are so important.

Police need more than a report saying that goods have been stolen. Useful information can include exact times and locations,

vehicle and trailer details, tracking data, CCTV, telephone numbers, email addresses, false paperwork, and descriptions of suspicious people or vehicles. We also need to get better at reporting attempted thefts, suspicious approaches, and fraud that was identified before the goods disappeared.

If somebody attempts to impersonate a legitimate carrier but the collection is stopped, it may feel as though there is nothing to report because no loss took place. But the same details could be used successfully against another company a few days later.

That information matters.

We need the data

As an industry, we still need a much more complete picture of what is being stolen, how it is being stolen, and where these incidents are happening. At the moment, too many thefts never make it into the available intelligence. A business may deal with a loss internally because the value falls below its insurance excess. It may decide not to make a claim, or it may simply not want the incident discussed more widely.

I understand the commercial concerns. Nobody wants to worry customers or damage their reputation. But keeping the information to ourselves does not help the wider industry, and ultimately it does not help the business that suffered the loss either. Whether an incident results in an insurance claim or not, the intelligence still matters. We need

companies to provide the relevant details to TIS so that the information can contribute to a more accurate understanding of the threat.

We have talked about the lack of data for long enough. We now need to get the information into one place and start using it. If we can bring together police, insurance,





Alarm systems

CYBER-SECURE LOCKS AND ACCESS-CONTROL PLATFORMS WITH UPTIME IN FOCUS

NO POWER OR CABLES NEEDED.
NO BATTERIES OR BATTERY REPLACEMENTS – EVER!



TRAILER



ROLLER-SHUTTER



CONTAINER



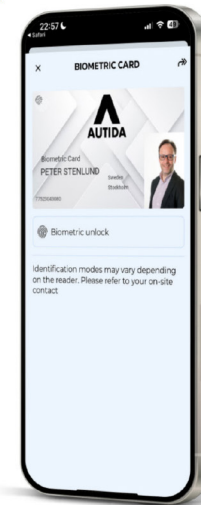
SWAP-BODY



CAR CARRIER



VAN



TAPA EMEA UK FREIGHT CRIME RISK & RESILIENCE
CONFERENCE · COVENTRY · 22 OCTOBER

LET'S TALK

Welcome! CEO and Management UK/Ireland.

'For me, TAPA EMEA's greatest value is its ability to bring the right people together and turn their combined knowledge into something practical. Within the Association, our diverse stakeholder membership all sees a different part of the problem.'

and industry incident data, while protecting commercially sensitive information, we will have a far more realistic picture of UK freight crime, which I believe is still massively underreported.

More incident intelligence will help operators and buyers make better decisions about routes, parking, vehicle security, and the protection required for particular products as well as their drivers.

It would also give us proper evidence when lobbying government for more secure parking investment or planning support, and create understanding at a political level for more policing resources, investment, and changes in national policy. Factual intelligence is a powerful tool to bring about positive change.

There is really no excuse not to share freight crime intelligence. Every report to TAPA EMEA remains anonymous. The identities of the victim of the crime or the person sharing the information are never disclosed. It's a change of mindset we need to achieve. If we only record the biggest insured losses or incidents that attract police attention, we will continue to underestimate the scale and nature of freight crime.

We cannot properly protect ourselves - or persuade other people to invest in the response - when we can only see part of the threat.

TAPA EMEA and UK law enforcement

TAPA EMEA is actively engaging with law enforcement across the EMEA region, offering free membership to qualifying law enforcement agencies and access to an international member network focused specifically on preventing freight crime. In the UK, both NaVCIS and OPAL are members and use TIS to support their work. I am keen to see more UK police officers and specialist units involved in freight crime investigations take advantage of the same opportunity, and I am making connections I hope will facilitate this.

Membership gives law enforcement specialists an opportunity for direct dialogue with manufacturers, logistics providers, insurers, security specialists, as well as other police professionals across the EMEA region. This can be especially valuable when an incident or investigation crosses a national border.

It should never be a one-way exchange. TAPA EMEA works best when industry and law enforcement learn from each other and build trusted relationships.

Where TAPA EMEA can make the biggest difference

For me, TAPA EMEA's greatest value is its ability to bring the right people together and turn their combined knowledge into something practical. Within the Association, our diverse stakeholder membership all sees a different part of the problem. TAPA EMEA brings those perspectives together and aligns them with its supply chain security Standards, incident intelligence, training, events, and international network. It can also help good practice to travel across borders. Something that works well in the Netherlands, Germany, Spain, or elsewhere may be just as relevant to a UK operation. In the same way, the experience of UK policing and industry can benefit other countries.

However, while TAPA EMEA can drive these initiatives, it needs members to be active and to realise the full benefits of membership. We need companies to join in relevant discussions, share appropriate information, and involve their operational teams as well as their security teams.

Bringing everyone together in Coventry

On 22 October 2026, we will host our TAPA EMEA UK Freight Crime Risk & Resilience Conference in Coventry, bringing law enforcement and industry together, and supported by the British International Freight Association (BIFA) and the Road Haulage Association (RHA).

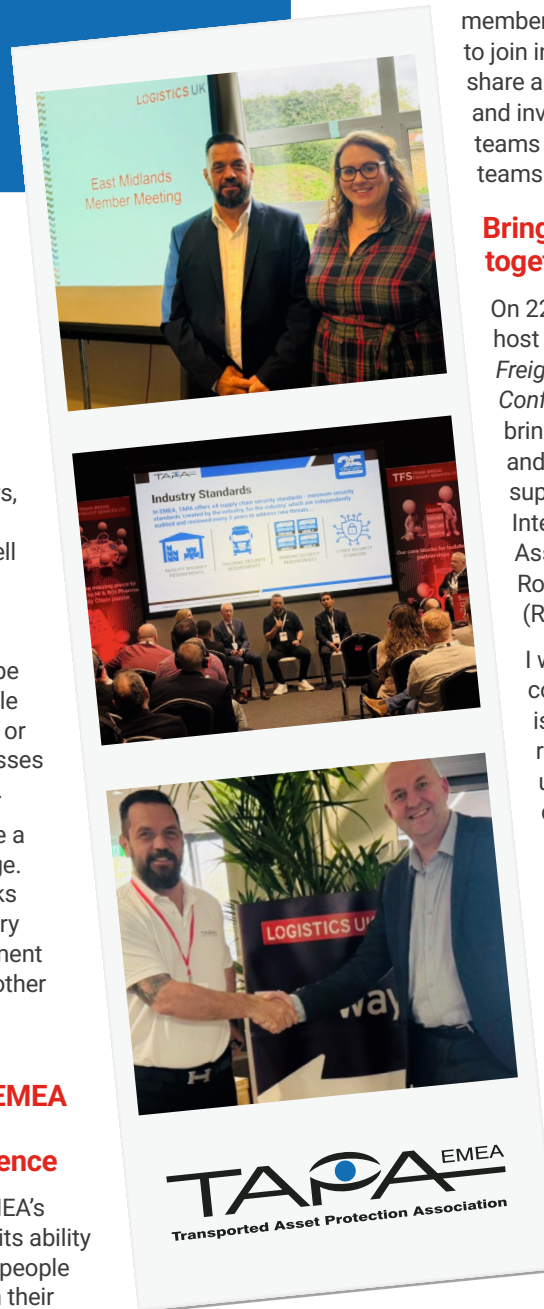
I want us to have honest conversations about what is working, where the gaps remain, and what each of us can do next. Freight crime cannot be solved by policing alone. And, it won't be solved by simply adding more equipment to vehicles or putting more conditions into transport contracts. It needs proper intelligence, recognised Standards, secure infrastructure, realistic planning, and genuine collaboration.

The UK has some extremely knowledgeable and committed people

working on this issue. Our challenge is to connect them, support them, and turn the current momentum into measurable improvements.

If we continue bringing together the people who buy transport services, provide transport solutions, protect goods, investigate crime, insure risk, and shape national policy, we can make the UK a much harder place for organised freight criminals to operate.

The momentum is there. Now we must quicken the pace of our actions.





SECURITY ESCORT



TRUCK.WATCH

GLOBAL COMPREHENSIVE SECURITY ESCORT SOLUTIONS



The Cargo Security Company delivers elite armed and unarmed escort solutions. Our qualified Risk Management Officers-former military and law enforcement-protect your shipments in fully equipped company vehicles. Backed by 24/7 real-time tracking, live streaming, and our triple-certified Security Operations Center (ISO 9001/27001, EN 50518).

- ✓ High-value cargo protection
- ✓ Cross-border escort operations
- ✓ Experienced risk management officers
- ✓ Visible & covert escort units
- ✓ Tailored reporting & analytics

FREIGHT CRIME IN THE UK

REGISTER NOW TO
JOIN US ON
22 OCTOBER...



TAPA EMEA UK Freight Crime Risk & Resilience Conference

CBS Arena - Coventry • 22 October 2026

Are your products moving in supply chains to, from, or within the United Kingdom? Or are you a transport or logistics provider responsible for ensuring the security and resilience of supply chain operations in the UK?

If you answered 'yes' to either of these questions, you won't want to miss TAPA EMEA's *UK Freight Crime Risk & Resilience Conference* in Coventry on 22 October 2026 to understand more about rising freight crime in the United Kingdom - and what can be done to make your supply chains more secure by increasing your understanding and management of known risks using readily available security solutions.

But – with over 200 delegate places already taken, you must register now while spaces are still available.

This must-attend event for UK supply chain security stakeholders is being supported by the British International Freight Association (BIFA) and the Road Haulage Association (RHA) who will also have senior representatives and member companies joining us in Coventry.

With the All-Parliamentary Group on Freight & Logistics estimating that freight crime now costs the United Kingdom economy and businesses over €800 million a year...

- Is industry doing enough to prevent organised crime groups and others from targeting supply chains?

- How are law enforcement agencies working to disrupt criminal organisations?
- And, what role do insurers have to play in making supply chains more resilient?

These questions and more will be on our agenda.

REGISTER NOW...

Important note: places at this event are strictly limited and only available on a first come, first served basis. All delegate places are subject to availability. Each TAPA EMEA member company can register **one** delegate as part of their membership benefits. And, as with all TAPA EMEA events, these registrations are subject to acceptance of TAPA EMEA's *No-Show Policy* (details available on the registration page). Additional delegate places can be purchased at €250.00 per delegate via info@tapaemea.org

Join us in Coventry on 22 October 2026 as the UK freight industry and law enforcement join forces in the fight against freight crime.

THORSTEN NEUMANN
President & CEO, TAPA EMEA

TAPA EMEA
Transported Asset Protection Association

BIFA
BRITISH INTERNATIONAL
FREIGHT ASSOCIATION

RHA





FAQs

What's on your mind?
This is your chance to
put your FSR, TSR, PSR
or CSS questions to
TAPA EMEA's Standards
& Training Team...

In this issue of *Vigilant*, TAPA EMEA's Standards & Training team discusses fence heights, walking distances, high-value cages, and FSR 2026 and TSR 2026 training courses ahead of the 2026 revisions of both Standards going 'live' in EMEA on 15 September...

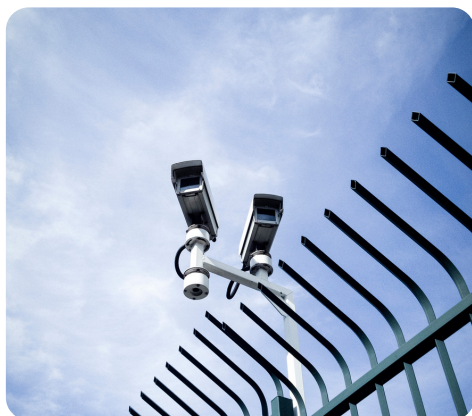
Question 1:

How should a facility's fence height be assessed when another structure could be used as a climbing aid?

Answer:

When assessing perimeter security, the relevant fence height should be measured from the highest point that could effectively be used as a climbing aid.

For example, if a wall behind a fence effectively reduces the usable fence height below the required level, the fence may need to be increased in height, or appropriate anti-climb protection may need to be extended to that location. The important consideration is therefore not simply the physical height of the fence itself, but the effective height available to a person attempting to overcome the perimeter.



Question 2:

In the TAPA Standards, is walking distance measured as a straight-line distance or the actual route people must take?

Answer:

Where a requirement is based on walking distance, the relevant measurement is the actual walking route, rather than the straight-line distance.

Physical barriers such as fencing can therefore influence the distance. For example, two locations may be relatively close together in a straight line, but if a fence requires a person to follow a defined route around the barrier, the longer walking distance is the relevant measurement.

An exception may also be considered where a parking space is permanently assigned to a specific, trusted vehicle, such as a management vehicle. In such a case, the vehicle should be known and assigned to an authorised and trusted individual.



Question 3:

Do high-value goods always have to be stored inside a High Value Cage?

Answer:

Not necessarily. Where goods such as large server racks cannot reasonably be accommodated inside a standard High Value Cage, an alternative secured storage arrangement may be possible.

A separate storage area could be designated specifically for a particular customer and reserved exclusively for that customer's goods. The customer would need to **formally agree** that its goods may be stored in this dedicated secured area. In such cases, the applicable security measures would be defined through the agreement between the customer and the warehouse operator or logistics provider. The key principle is therefore that an alternative storage arrangement must provide an appropriate level of security and be **formally agreed with the customer**.



Question 4:

What should companies consider regarding the updated FSR 2026 and TSR 2026 TAPA Standards and the transition to the new requirements?

Answer:

The **2026 Standards officially come into effect on 15 September 2026**. Until 14 September 2026, certifications can still be conducted against the 2023 Standards. From 15 September onwards, new certifications must be conducted against the applicable 2026 Standard.

The transition also affects auditors. To conduct audits against the 2026 Standards, auditors need to obtain the relevant **Authorized Auditor (AA) qualification** through successful completion of the corresponding training.

TAPA EMEA has made the **FSR 2026 and TSR 2026 Standards** available on its website, including a marked-up version showing the changes compared with the previous 2023 editions. Members planning new certifications or audits later in 2026 should therefore take the transition timeline into account and ensure that their sites, procedures, and relevant personnel are prepared to meet the requirements of the new Standards.



Question 5:

Our current Authorized Auditor (AA) will be leaving the company and his replacement can only attend the 2026 training. Is this acceptable if we are certified with the 2023 Standard version?

Answer:

Yes. There is no issue if the replacement completes the 2026 version of the relevant TAPA training. Training for a newer or revised version of the Standard also covers the knowledge required for previously issued versions. Therefore, an individual trained on the 2026 Standard is considered trained for the earlier Standard versions as well.

A new training course is only required where the individual's most recent training is based on the 2023 Standard, but the audit or certification will be conducted against the 2026 Standard. In this case, the individual must complete the relevant 2026 training before conducting the certification activity.

This approach allows companies to replace their AA without creating an unnecessary training gap during the transition from the 2023 to 2026 versions of the Standards.



Question 6:

Can we complete the 2026 Standards' training in a language other than English from 1 September 2026?

Answer:

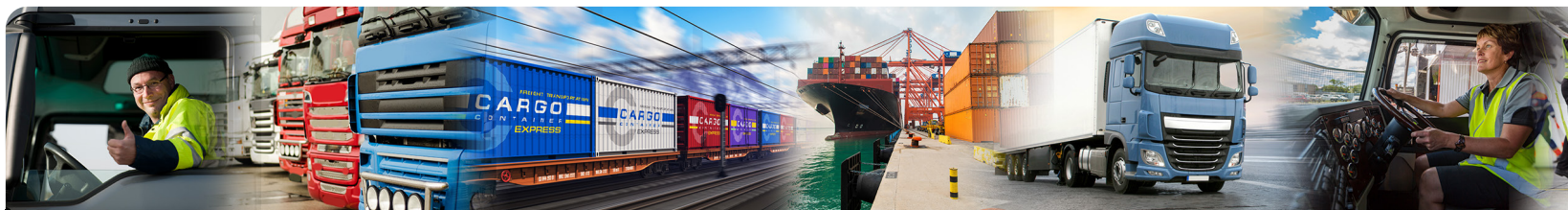
Initially, the 2026 training programmes will only be available in English and members will be able to book FSR 2026 and TSR 2026 trainings from 1 September. TAPA EMEA will begin translating the training materials immediately afterwards. The translation, preparation, and verification process is expected to take approximately 2-3 months before additional language versions can be launched.

French, Italian, Spanish, and Polish versions of the Standards (not necessarily in this order) will be the first languages prioritised for translation. We therefore ask members to plan their training activities accordingly and appreciate their understanding while the additional language versions are being prepared.



FSR & TSR TRAINING COURSES

Look out for TAPA EMEA's communication on 1 September 2026 on registering for your FSR 2026 & TSR 2026 training courses...



TAPA'S LATEST FSR, TSR & PSR STANDARDS' CERTIFICATIONS

SECURITY LEADERS

MONTHLY STATISTICS

**TOTAL
NUMBER OF
CERTIFICATIONS**
70

**NUMBER OF
COMPANIES
CERTIFYING**
46

**COUNTRIES IN
EMEA RECORDING
CERTIFICATIONS**
20

TAPA EMEA
Transported Asset Protection Association

The following companies and locations were audited by one of TAPA EMEA's approved Independent Audit Bodies (IABs) or, in the case of Class 'C' or Level 3 certifications for FSR and TSR respectively, may have been completed by an in-house TAPA EMEA-trained person. Plus, a list of our latest PSR Partners and certifications.

FSR – EUROPE, MIDDLE EAST & AFRICA REGION

	COMPANY NAME	CITY	COUNTRY	CLASS
FSR	A.P. Moller - Maersk AS	Alcala de Henares	Spain	C
FSR	A.P. Moller - Maersk AS	Barcelona	Spain	C
FSR	Albini E Pitigliani S.P.A.	Vignate	Italy	A
FSR	Amazon Com INC	Birmingham	United Kingdom	A
FSR	Amazon Com INC	Nottingham	United Kingdom	A
FSR	Amazon Com INC	Rochester	United Kingdom	A
FSR	Amazon Com INC	Dartford	United Kingdom	A
FSR	Amazon Com INC	Dunstable	United Kingdom	A
FSR	Amazon Com INC	Dunfermline	United Kingdom	A
FSR	Amazon Com INC	Fara in Sabina	Italy	A
FSR	ATC Part of Arvato	Slough	United Kingdom	A
FSR	CEVA Logistics	Waalwijk	Netherlands	A
FSR	CEVA Logistics	Doncaster	United Kingdom	A
FSR	Conectiv Polska Sp. z o.o.	Józefostaw	Poland	C
FSR	DHL Express	Valence	France	C
FSR	DHL Express	Kurmach	Germany	C
FSR	DHL Express	Straubing	Germany	C
FSR	DHL Express	Tuntenhausen	Germany	C
FSR	DHL Express	Brnik	Slovenia	A
FSR	DHL Express	Izmir	Turkey	A
FSR	DHL Express	Istanbul	Turkey	B
FSR	DHL Express	Istanbul	Turkey	A
FSR	DHL Express	Marignane cedex	France	A
FSR	DHL Express	Rumilly	France	A
FSR	DHL Express	Napoli	Italy	A
FSR	DHL Express	Peggau	Austria	A
FSR	DHL Express	Klagenfurt	Austria	A
FSR	DHL Freight Germany Holding GmbH	Vilnius	Lithuania	C
FSR	DHL Global Forwarding Italy SPA	Pozzuolo Martesana	Italy	C
FSR	DHL Global Forwarding Italy SPA - , Italy	Fiumicino	Italy	C
FSR	DPD (Nederland) B.V.	Geertruidenberg	Netherlands	C
FSR	DPD (Nederland) B.V.	Geertruidenberg	Netherlands	C
FSR	DSV A/S	Leixlip	Ireland	A
FSR	Eurohub Pharma Logistics S.A.	Keratea	Greece	A
FSR	FIEGE Logistik Stiftung & Co. KG	Zulpich	Germany	C
FSR	FIEGE Logistik Stiftung & Co. KG	Hamburg	Germany	C
FSR	FoodLink SA	Aspropyrgos	Greece	A
FSR	Freschi & Schiavoni SRL	Vignate	Italy	A
FSR	Geodis FF Germany & Co KG	Rhijnauwen 4, Almere	Netherlands	C
FSR	Geodis FF Germany & Co KG	Wittevrouwen 21, Almere	Netherlands	C
FSR	Geopost Espana SL	Murcia	Spain	C
FSR	Ingram Micro Europe b.v.	Houdeng-Goegnies	Belgium	C
FSR	NX Lifestyle Logistics France SAS	Croissy-Beaubourg	France	A
FSR	Orphee Beinoglou - Stroom Global Supply Chain Solutions S.A.	Elefsina	Greece	A
FSR	Poste Italiane Spa	Elmas	Italy	A
FSR	Trans X Tar S.L.	Riba-roja de Túrria	Spain	C
FSR	trans-o-flex Express GmbH & Co. KGaA	Kassel	Germany	C
FSR	UPS Healthcare Hungary Zrt	Budaros	Hungary	A



...HELPING TO IDENTIFY LEADERS IN SUPPLY CHAIN SECURITY



TSR – EUROPE, MIDDLE EAST & AFRICA REGION

	COMPANY NAME	COUNTRY	LEVEL
TSR	AIT Home Delivery Deutschland GmbH - Lehrte	Germany	Level 3 / Category - Small
TSR	Anwil Transport Sp. z o.o. Sp.k. - Suchy Las	Poland	Level 1,2 / Category - Large
TSR	Arcese Trasporti S.P.A. - Basiano	Italy	Level 1 / Category - Small
TSR	Atlas Imobiliare Srl - Alba Iulia	Romania	Level 3 / Category - Large
TSR	Autotrasporti Moretti Srl - Porto Sant'Elpidio	Italy	Level 1 / Category - Small
TSR	B.O.R.Y.S. Logistic Sp. z o.o. - Gostyn	Poland	Level 1 / Category - Small
TSR	Delta Transportni Sistem - D.T.S. Doo Beograd - Nova Pazova	Serbia	Level 1 / Category - Small
TSR	Dual Logistic Ltd - Burton on Trent	United Kingdom	Level 3 / Category - Large
TSR	Eurohub Pharma Logistics S.A. - Keratea	Greece	Level 1 / Category - Small
TSR	Firma T.H.U. i S. Leszek Flak - Tryńcza	Poland	Level 1 / Category - Small
TSR	Interfjord A/S - Roslev	Denmark	Level 1 / Category - Small
TSR	Janusz Kmoch - Somianka	Poland	Level 1 / Category - Small
TSR	King com transs international Srl - Volovăț	Romania	Level 1 / Category - Small
TSR	Mesaroli Logistica S.p.A. - Senec	Slovakia	Level 1 / Category - Over-Large
TSR	SAF Srl - Gricignano di Aversa	Italy	Level 1 / Category - Medium
TSR	SC Transsami SRL - Suceava	Romania	Level 1 / Category - Small
TSR	SGL Logistics - Roscommon	Ireland	Level 3 / Category - Small
TSR	SIT Expedicion Arte Y Seguridad SL - Coslada	Spain	Level 3 / Category - Small
TSR	SIT Grupo Empresarial SL - Coslada	Spain	Level 3 / Category - Small
TSR	Velox Express GmbH - Wien	Austria	Level 1 / Category - Small
TSR	Voge Transport Ltd - Crewe	United Kingdom	Level 1 / Category - Small

PSR/PPD – EUROPE, MIDDLE EAST & AFRICA REGION

	COMPANY NAME	CITY	COUNTRY	PSR / PPD
PSR/PPD	Fabb Park	Hauconcourt	France	PPD



TAPA TALKS PODCAST

The inside track
on supply chain
security

EPISODE 3
OUT NOW...

TAPA EMEA'S THORSTEN
NEUMANN & GUESTS

FIGHTING
FREIGHT FRAUD
& FAKE
CARRIERS

DOWNLOAD & LISTEN NOW...





TOTALLY TAPARIZED!

Every year, TAPA EMEA's work to support members using our supply chain security standards, the development of our training programme, the growth of our supply chain intelligence platform, and our networking events and security insights, are delivered with the support of our *Premier Partners*, all leading providers of supply chain security products and services – and all strongly committed to advancing the resilience of our members' supply chains.

We thank all our 2026 *Premier Partners* for their support and for being TOTALLY TAPARIZED.



PARTNERS IN SUPPLY CHAIN SECURITY & RESILIENCE