



TT Club Loss Prevention

September 2026

Supply chain security bulletin

What's inside?

Fusible and the evolution of data-led security in road freight

Copper theft risk rising across global supply chains

Trailer theft at a secure port facility

Shifting Carrier Identities: A Persistent Threat to Logistics Integrity

Contents

- 03 Foreword
- 04 Securing the supply chain: the critical role of container chassis security
- 06 Fusable and the evolution of data-led security in road freight
- 08 Advancing secure truck parking: an interview on risk, resilience and continuous improvement
- 10 Copper theft risk rising across global supply chains
- 12 Trailer theft at a secure port facility
- 14 Shifting carrier identities: a persistent threat to logistics integrity



Disclaimer

The information contained in this publication has been compiled from various sources. TT Club, its managers and all other contributors do not accept responsibility for loss or damage which may arise from reliance on the information provided.

Copyright © Through Transport Mutual Services (UK) Ltd 2026. All rights reserved. Users of this briefing may reproduce or send it verbatim only. Any other use, including derivative guidance based on this briefing, in any form or by any means is subject to prior permission in writing from Through Transport Mutual Services (UK) Ltd.

Supply chain security bulletin

This bulletin considers all aspects of supply chain security, highlighting TT Club claims statistics along with a range of other industry data offering an invaluable insight into the current risks facing those tasked with managing security through the supply chain. The Club has produced several reports and guidance documents related to this area of risk across many media platforms.

This bulletin presents a selection of TT Club content and publications as well as highlighting collaborative work undertaken with other like-minded organisations in this space.

The entire library of TT Club's loss prevention guidance can be found at www.ttclub.com/loss-prevention. Please email us at riskmanagement@ttclub.com or get in touch with your usual contact should you have any queries, ideas or suggestions.

Foreword

The themes running through this edition of the TT Club Supply Chain Security Bulletin are clear: cargo criminals are becoming more organised, more technologically capable and increasingly adept at exploiting weaknesses in both physical and procedural controls. At the same time, the industry has access to more data, better intelligence and stronger collaborative networks than ever before. The challenge for supply chain stakeholders is to ensure that risk management practices evolve at least as quickly as the threats they face.

This edition explores how technology, operational discipline and industry collaboration can strengthen supply chain resilience. We examine the growing role of data-led intelligence through an analysis of Fusable's carrier risk monitoring capabilities, while also considering how advanced asset tracking solutions are transforming visibility and security for intermodal equipment. These developments demonstrate how access to timely, actionable information can help organisations identify emerging threats, improve decision-making and reduce exposure across increasingly complex transport networks.

The bulletin also highlights the continued importance of fundamental security controls. An interview focusing on secure truck parking reinforces that effective security is not achieved through infrastructure alone, but through continuous improvement, rigorous testing and close cooperation between operators, authorities and drivers. Similarly, our review of rising copper theft risks demonstrates how organised criminal activity continues to adapt to changing market conditions, requiring layered controls that address both physical theft and fraud-enabled attacks.

Real-world loss experience remains one of the most valuable sources of learning. The case study involving the theft of a high-value trailer from a secure port environment illustrates how sophisticated criminals can exploit weaknesses in information security, verification procedures and tracking arrangements.

Alongside this, our examination of reincarnated carriers highlights the growing threat posed by deceptive business practices that undermine trust and integrity throughout the logistics sector. Together, these examples underline the need for robust due diligence, effective authentication processes and a sceptical approach to anomalies that may indicate criminal activity.

While the methods employed by criminals continue to evolve, the underlying lesson remains consistent: security is most effective when it combines people, processes and technology within a culture of continuous vigilance. By sharing insight, practical guidance and lessons learned from across the industry, we hope this bulletin assists organisations in strengthening their defences and enhancing the resilience of the global supply chain.

Joshua Finch
TT Club Loss Prevention



Securing the supply chain: the critical role of container chassis security

In today’s global logistics landscape, the security and visibility of supply chain assets have never been more vital. As the backbone of intermodal transport, container chassis play a pivotal role in ensuring the smooth movement of goods across continents. Yet, with increasing complexity and heightened customer expectations, traditional methods of managing and securing these assets are no longer sufficient. The integration of advanced asset tracking solutions, such as BlackBerry Radar, is transforming the way organisations safeguard their fleets, optimise operations, and respond to the ever-evolving demands of the supply chain.

The challenge: visibility and security in a dynamic environment

Container chassis are essential, yet inherently vulnerable, components of the supply chain. Historically, operators have relied on manual yard checks, paper-based reporting, and delayed electronic data interchange (EDI) feeds to monitor their fleets. These methods are not only labour-intensive but also prone to inaccuracies and delays, leading to operational inefficiencies and increased risk. The inability to locate specific units quickly, assess their status in real time, or ensure compliance with regulatory standards exposes companies to potential losses, compliance breaches, and customer dissatisfaction.

The solution: purpose-built asset tracking

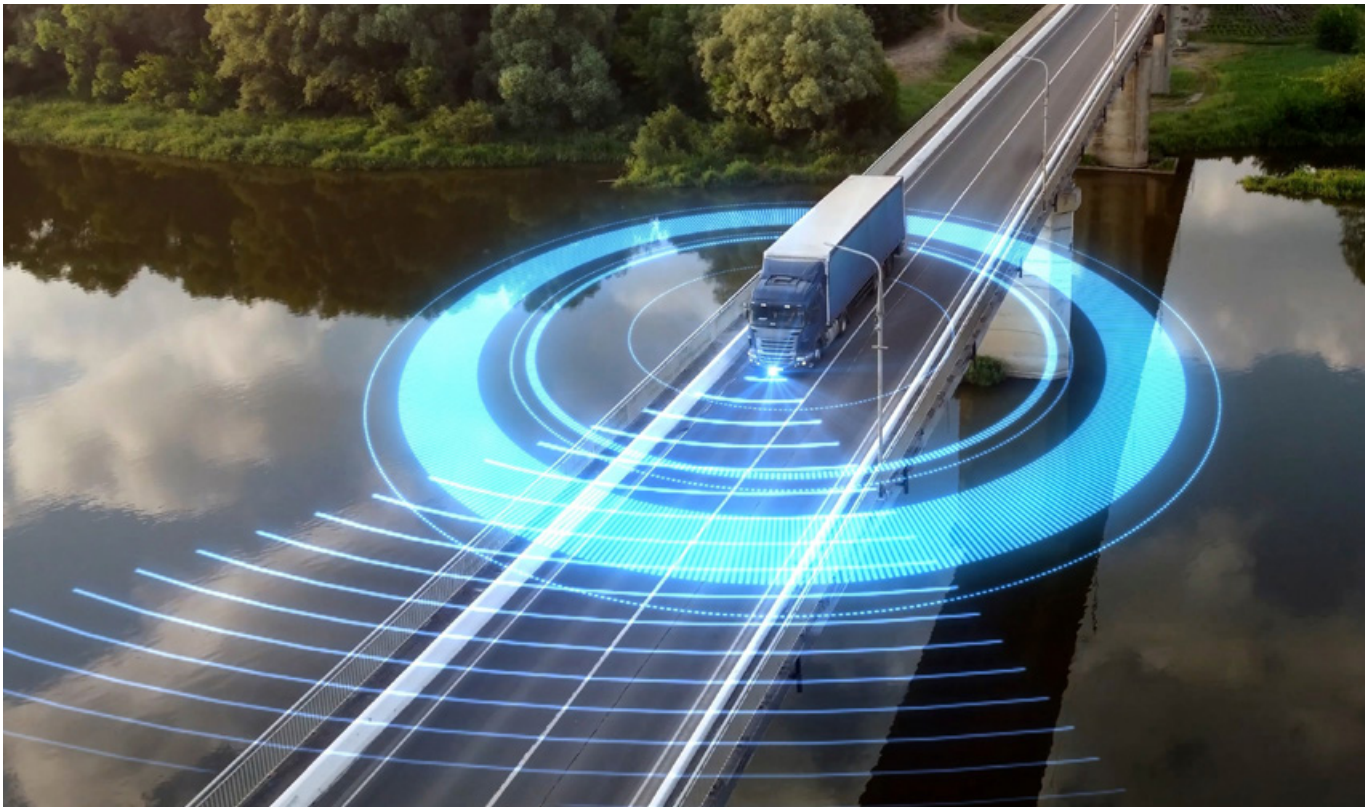
The advent of purpose-built asset tracking solutions marks a significant leap forward in supply chain security. BlackBerry Radar, for example, is engineered specifically for non-powered assets such as chassis, containers, trailers, and railcars. Its ruggedised sensors and intuitive reporting platform provide actionable, real-time data that drive business efficiency and enhance security. Installation is straightforward – often completed in under ten minutes – and the system boasts a low total cost of ownership, making it accessible for fleets of all sizes.



Key features enhancing chassis security

Modern asset tracking platforms offer a suite of features designed to address the unique challenges of container chassis management:

- **Accurate GPS location and mileage tracking:** Real-time location data ensures that every chassis can be pinpointed instantly, reducing the risk of loss or theft and enabling rapid response to security incidents.
- **Trip reporting and start/stop alerts:** Automated logs of chassis movements provide a transparent record of asset utilisation, supporting both operational efficiency and compliance.
- **Impact and tamper detection:** Sensors detect both horizontal and vertical impacts, as well as unauthorised access or tampering, alerting operators to potential security breaches.
- **Container on/off sensing:** For intermodal chassis, knowing precisely when a container is mounted or dismounted is crucial for asset management and theft prevention.
- **Custom geofences and alerts:** Operators can set up location-based alerts, ensuring that assets remain within authorised zones and are quickly flagged if they deviate.



Operational benefits: efficiency meets security

The deployment of advanced tracking solutions delivers tangible operational benefits that go hand in hand with enhanced security:

- **Automated event capture:** By eliminating manual processes, companies achieve real-time visibility into equipment location and usage, reducing errors and delays.
- **Greater yard efficiency:** Digital tracking replaces time-consuming manual audits, freeing up personnel and reducing the margin for error.
- **Improved network balancing:** Centralised visibility enables more effective asset distribution, ensuring that chassis are available where and when they are needed.
- **Enhanced compliance management:** Maintenance alerts and GPS-based tracking support regulatory inspection readiness, ensuring that only compliant chassis are in service.
- **Customer transparency:** Real-time data empowers customers and drivers with insights into asset location and dwell times, strengthening relationships and service delivery.

Strategic value: agility and future-proofing

Beyond immediate operational gains, the integration of platforms like BlackBerry Radar positions organisations for long-term success. The open API and sensor gateway capabilities allow for seamless integration with existing systems and future expansion into areas such as tyre pressure or brake monitoring. This flexibility ensures that the technology remains relevant as business needs evolve.

The experience of Direct ChassisLink Inc. (DCLI), a major player in the US intermodal transport sector, illustrates these benefits vividly. By piloting and then scaling the deployment of BlackBerry Radar across a portion of its fleet, DCLI achieved significant improvements in data accuracy, yard efficiency, compliance, and customer service. The ability to customise the platform to specific operational requirements further reinforced the value of selecting a partner capable of deep integration and ongoing innovation.

Looking ahead: the future of secure, responsive supply chains

As the freight industry continues to grapple with challenges such as driver shortages, rising costs, and supply chain disruptions, the need for advanced asset visibility and enhanced fleet management solutions has never been greater. The data captured through modern tracking platforms is not just about knowing where assets are – it is about empowering organisations to make smarter, faster decisions that protect their assets, serve their customers, and drive business growth.

In conclusion, securing the supply chain begins with securing its most fundamental assets. By embracing purpose-built tracking solutions, logistics providers can transform container chassis from potential vulnerabilities into pillars of operational excellence and strategic advantage.



Michael Dunning
Senior Portfolio Underwriter

Michael joined the TT Club in our London office in 2014 where he was responsible for Underwriting our Middle Eastern, African and French members. In 2022, Michael moved to our New Jersey office to work as an Underwriter for the Club's Americas region and is now a Senior Portfolio Underwriter.

Fusable and the evolution of data-led security in road freight

Introduction

The increasing sophistication of freight crime, coupled with growing legal and financial exposure across the supply chain, is driving renewed focus on due diligence and carrier verification. Within this context, technology providers that connect fragmented public, regulatory and proprietary data with historical and analytical context are playing an increasingly central role. Among these, Fusable, through its Central Analysis Bureau (CAB) platform, has established itself as a prominent provider of motor carrier risk intelligence for the road freight and insurance sectors.

Drawing on extensive datasets and analytical techniques, Fusable's solutions are designed to enable insurers, freight brokers and shippers to better understand who they are doing business with, identify risk indicators that may otherwise remain hidden, and place current findings in historical context.

What does CAB provide to the market?

Fusable's core proposition lies in aggregating and structuring publicly available data relating to motor carriers, transforming disparate regulatory and public motor-carrier data into coherent risk intelligence by adding historical context, relationship insights, CAB-enhanced analytics, and other Fusable data signals. The CAB platform is widely used across the United States insurance market, with high levels of penetration among commercial motor insurers, many of whom require its use as part of underwriting processes.

At its foundation, the CAB platform integrates multiple data sources, including roadside inspection data, regulatory filings, registration records and, where captured during inspections, shipper information recorded from shipping documents. While each of these datasets is individually accessible, their raw formats can be difficult to interpret. Where available and authorised, telematics shared from TruckerCloud can enable CAB to display mileage, location, route, garaging and driving-behaviour insights.

A key feature is the calculation and monitoring of Behavior Analysis and Safety Improvement Categories (BASICs), inspection and violation histories and related safety performance. These indicators are widely used within the US regulatory framework and are regarded as a core component of carrier risk assessment.

“
The CAB platform processes a high volume of data, including tens of thousands of roadside inspections conducted weekly across the United States.
”

How CAB maps carrier relationships to strengthen due diligence

A defining capability of the CAB platform is its ability to identify and map relationships between entities that may not be immediately apparent. CAB analyses shared attributes such as addresses, telephone numbers, email domains, representatives, historical records and equipment or Vehicle Identification Numbers. Recent enhancements also incorporate Fusable financial-activity data from Uniform Commercial Code (UCC) filings, where available, helping evidence relationships among fleets by linking financial transaction data or equipment financing data.

This approach is particularly relevant in the context of fraudulent or deceptive practices, where individuals may establish multiple companies, sometimes sequentially, to obscure past performance or regulatory interventions.

One application of this capability is the identification of businesses that attempt to obscure their identity through closure, re-emerging under a new identity following safety enforcement actions or other issues. While the platform does not assert wrongdoing; it flags potential connections and encourages further investigation. This distinction is important, as legitimate business restructuring can create similar data patterns.

From a risk management perspective, such visibility allows insurers and freight brokers to move beyond static compliance checks and undertake a more dynamic assessment of counterparties.

Monitoring risk across the carrier life cycle

In addition to initial screening, the CAB platform supports ongoing monitoring through CAB List. Users can establish watchlists and receive alerts when predefined thresholds or changes occur.

These alerts may include changes in contact details, safety scores, new inspection findings or the emergence of new relationships with other entities. Such changes can serve as early warning indicators of increased risk, prompting users to review their exposure.

The ability to monitor carriers on an ongoing basis reflects a broader shift in risk management practice. Historically, many organisations relied on point-in-time verification, confirming regulatory compliance at onboarding and then assuming continued suitability. However, evolving legal expectations, particularly in the United States, are placing greater emphasis on ongoing due diligence.

This development is partly driven by litigation trends, including large liability awards, which increasingly draw multiple parties in the logistics chain into disputes. As a result, there is growing scrutiny of the decision-making processes used to select and retain carriers.

Supply chain security risks

Freight fraud, including double brokering and cargo theft, remains a persistent concern across the road transport sector. CAB's data-driven approach provides tools to mitigate these risks by improving visibility and enabling earlier detection of anomalies.

Patterns such as repeated changes in company identity, shared infrastructure or equipment, financial relationships and discrepancies in operational data can all signal elevated risk. By consolidating these indicators into a single analytical environment,



the CAB platform allows users to identify concerns that may not be evident through manual processes.

Crucially, CAB is not limited to active entities. Historical records, including information on inactive or dissolved companies, are retained and incorporated into analysis. This historical perspective enhances the detection of recurring patterns, particularly where entities attempt to evade scrutiny by ceasing operations and re-emerging under new registrations.

The use of inspection data also provides insight into operational behaviour, including geographic movement patterns and shipper interactions, further enriching the risk profile.

Data quality, scale and limitations

The CAB platform processes a high volume of data, including tens of thousands of roadside inspections conducted weekly across the United States. This volume supports statistically meaningful analysis at a macro level, even though data availability may vary for individual carriers.

As with any data-driven system, limitations exist. Inspection frequency can differ by region, and smaller operators may have limited data footprints. However, the platform mitigates these gaps by incorporating multiple data sources, historical records and focusing on relational indicators rather than relying solely on volume-based metrics.

The broader regulatory environment is also evolving. Authorities continue to invest in improved data collection and identity verification processes, with new registration systems and automated inspection technologies under development. These initiatives are expected to enhance both the timeliness and completeness of available data, further strengthening analytical tools built upon these foundations.

Adoption across the logistics and insurance ecosystem

Although initially developed for the insurance sector, the CAB platform is increasingly used across a wider range of stakeholders, including freight brokers, shippers, leasing companies and factoring firms. This reflects the interconnected nature of supply chain risk, where vulnerabilities in one area can rapidly impact others.

The CAB platform's widespread adoption is underpinned by its perceived reliability and the practical value it delivers. Users often integrate the data into core decision-making processes, including underwriting, carrier selection and portfolio monitoring.

In some cases, the absence of such data is seen as a significant operational gap, highlighting the extent to which data-driven tools have become embedded in modern risk management practices.

Conclusion

Fusable's CAB platform represents a broader shift towards intelligence-led risk management in road freight and logistics. By transforming complex and fragmented datasets into structured, actionable insights, it enables stakeholders to make more informed decisions across the carrier lifecycle.

As supply chains become more complex and regulatory expectations continue to evolve, the importance of robust due diligence and ongoing monitoring is likely to increase. In this environment, platforms that can illuminate hidden relationships, track emerging risks and provide timely alerts will play an increasingly critical role.

For insurers, freight brokers and other logistics stakeholders, the adoption of such tools is no longer solely a matter of operational efficiency. It is becoming an essential component of managing exposure, maintaining resilience and safeguarding the integrity of the supply chain.

FUSABLE



Josh Finch
Logistics Risk Manager

Josh is a Logistics Risk Manager for TT Club's Loss Prevention department. Josh joined TT Club in 2023 having 15 years of experience in the logistics industry in various operational and project management roles. He has extensive experience managing warehouses and running road freight transport operations. He is an International CPC qualified Transport Manager.

Advancing secure truck parking: an interview on risk, resilience and continuous improvement

In response to rising cargo theft across European supply chains, secure truck parking has emerged as a critical risk control measure. However, as industry experience continues to demonstrate, effective security extends far beyond infrastructure. It requires continuous testing, operational discipline and close collaboration across multiple stakeholders.

The following interview explores these themes through a discussion between TT Club and Thierry Roger of Bapaume Truck House, drawing out practical insights on how high-security facilities can strengthen supply chain resilience while improving driver welfare.

Context and definitions

From your perspective, how significant is the role of secure parking in addressing cargo theft across Europe?

Secure parking plays a fundamental role because the majority of cargo theft incidents still occur when vehicles are parked in unsecured environments. Across both the United Kingdom and mainland Europe, criminals actively target trucks parked on roadside verges, in industrial estates or in poorly monitored areas. This makes parking choice one of the most important decisions a driver or operator can make.

How would you define a truly secure truck parking facility?

A secure facility is one that combines infrastructure, procedures and active management. Industry certifications such as the Transported Asset Protection Association (TAPA) Parking Security Requirements (PSR) and European standard for Safe and Secure Truck Parking Areas (SSTPA) provide a useful framework. However, certification alone is not sufficient. Operators must develop additional controls and continuously assess whether the system remains effective in practice.

Risks and consequences

From an insurance and risk management perspective, why is unsecured parking such a persistent issue?

The core issue is accessibility. Unsecured vehicles offer criminals a low-risk, high-reward opportunity. Methods such as curtain slashing can be executed quickly, often without immediate detection. Even where contractual liability is limited, the downstream consequences are significant, including reputational damage, operational disruption and strained customer relationships. The financial impact is therefore broader than the value of the stolen cargo itself.



Thierry Roger
CEO, Truck House

Thierry has over eight years of experience managing high-security truck parking operations in France, specialising in cargo theft prevention, operational security and driver safety. He has implemented advanced security measures, conducted risk assessments and security audits, and worked closely with logistics stakeholders, law enforcement and security professionals to strengthen supply chain security and support secure parking and driver wellbeing initiatives across Europe.



Is fraud now a greater concern than physical theft?

Fraud has received considerable attention, but physical theft remains the dominant issue. Opportunistic and organised criminals continue to exploit weaknesses in parking security. As long as unsecured parking remains widely used due to capacity constraints or operational pressures, this risk will persist.

Security management in practice

You have described security as a “living process”. What does that mean in practice?

It means that security cannot be static. Criminal behaviour evolves, so defensive measures must evolve as well. In practice, this requires continuous testing of systems and personnel. For example, conducting unannounced intrusion tests or reviewing surveillance coverage to identify blind spots. Even highly secure facilities can develop vulnerabilities over time if vigilance declines.

Have you encountered situations where your own controls failed?

Yes, and those situations are extremely valuable from a learning perspective. During internal testing, there were occasions where it was possible to enter the site without detection. These exercises revealed weaknesses in guard performance and surveillance monitoring. As a result, security providers were changed and procedures strengthened. This reinforces the principle that effective security depends as much on people and behaviour as it does on physical infrastructure.

How do you address risks during site expansion or change?

Periods of construction or expansion can introduce temporary vulnerabilities. These must be identified and managed proactively through additional controls, such as restricted access zones, enhanced monitoring and revised patrol routines. The key is to anticipate where weaknesses may emerge rather than waiting for an incident to occur.

Accreditation and operational reality

What role does accreditation play in your operations?

Accreditation is essential because it provides credibility to customers, insurers and transport operators. Certifications such as TAPA PSR Level 1 and European Union (EU) Platinum standards demonstrate that a facility meets recognised benchmarks. However, accreditation is only the starting point. Operators must go beyond these requirements to address site-specific risks and emerging threats.

Would it be fair to say that accreditation is necessary but not sufficient?

That is correct. Certification establishes baseline standards, but real security performance depends on how those standards are implemented and improved over time. Operators should aim to exceed minimum requirements rather than simply comply with them.

Collaboration with authorities

How important is engagement with local authorities and law enforcement?

It is critically important. A secure parking facility does not operate in isolation. Collaboration with local authorities can support policies that reduce roadside parking, while engagement with law enforcement enhances deterrence through visible patrols and rapid response.

Have you observed measurable benefits from this collaboration?

Yes. Following the introduction of a secure parking facility and coordinated engagement with local authorities and law enforcement, cargo theft in the surrounding area decreased. While it is difficult to attribute this entirely to one factor, the presence of a controlled environment and increased visibility of enforcement activity contributed to a measurable reduction.

Does this eliminate theft risk in the region?

Not entirely. What often occurs is displacement, where criminal activity shifts to less secure locations. This highlights the need for wider adoption of secure parking across key transport corridors.

Driver welfare and its impact on security

Driver welfare is often discussed separately from security. How do you see the relationship between the two?

They are closely linked. A fatigued or stressed driver is more likely to make poor decisions, including parking in unsafe areas. By improving driver welfare, operators can indirectly enhance security outcomes.

What practical measures support this?

Providing clean facilities, access to food, rest areas and opportunities for social interaction can make a significant difference. Creating an environment where drivers feel safe and valued encourages them to use secure facilities consistently. Engagement with drivers is also essential, as it allows operators to understand their needs and adapt services accordingly.

Best practice and industry implications

Based on your experience, what are the key principles for effective secure parking?

The most important principle is continuous improvement. Security systems must be regularly tested and updated. Accreditation should be treated as a framework rather than a final objective. Collaboration with authorities enhances deterrence, and driver welfare should be integrated into security planning.

What does this mean for the wider industry?

For logistics operators and cargo owners, it means prioritising secure parking within route planning and operational decision-making. For insurers and risk specialists, it reinforces the importance of promoting best practice and supporting infrastructure development. Ultimately, reducing cargo theft requires a coordinated effort across the entire supply chain.

Conclusion

The discussion demonstrates that secure truck parking is not a static solution, but an evolving discipline that requires proactive management, stakeholder collaboration and a strong focus on human factors. While infrastructure and accreditation provide a necessary foundation, sustained reduction in cargo theft depends on continuous testing, operational vigilance and the integration of driver welfare considerations.

As supply chains become increasingly complex and risk exposure grows, the role of secure parking will continue to expand. Operators that embrace a dynamic, intelligence-led approach to security are likely to play a central role in shaping more resilient and secure logistics networks across Europe.

Copper theft risk rising across global supply chains

Copper theft has shifted over the past decade from an opportunistic crime to a persistent supply chain threat, driven by commodity value, organised criminal involvement, and vulnerabilities in transport and storage controls. TT Club's longitudinal claims experience indicates a marked and accelerating rise in both incident frequency and financial impact, reinforcing that copper should be treated as a high-risk cargo across multiple modes and locations.

The trend matters because the loss is rarely limited to the stolen cargo alone. Theft can trigger delay, contractual dispute, reputational harm, and wider operational disruption, particularly where copper is embedded in critical infrastructure and industrial supply chains. As a result, controls that are adequate for routine cargo may be insufficient for copper movements, especially when market conditions increase criminal incentive.

Why copper theft is increasing

TT Club claims data for 2016–2025 shows a clear upward trajectory in copper theft incidents. Recorded cases rise from 2 incidents in 2016 to 37 in 2025, representing more than an eighteenfold increase over the period. Intermediate years show intermittent spikes aligned with emerging hotspots and heightened market values, including 2017 with 10 claims and 2020 with 17 claims. The steepest recent acceleration is evident between 2022 with 21 claims and 2023 with 29 claims, followed by further growth by 2025.

The pattern is consistent with a market-influenced theft commodity. The draft data links theft frequency and cost to global copper pricing, with higher average pricing years, including 2021, 2022, 2024, and 2025, aligning with increased theft activity. In practical terms, rising prices amplify criminal incentive and can cause rapid shifts in targeting behaviour where supply chain controls are weakest.

It is also significant that TT Club's 2025 data identify copper as the single most commonly stolen cargo. This finding supports treating copper as an elevated-risk exposure rather than as a routine commodity shipment, with commensurate expectations around due diligence, route control, and monitoring.

Where risk sits in the supply chain

Copper theft risk is most visible during transport, but the exposure extends beyond the transport leg. Copper is integral to construction, energy networks, and broader infrastructure systems, and the draft highlights that theft increasingly occurs not only in transit or storage but also at yards, terminals, warehouses, and production facilities.

“Several recurring weaknesses can undermine otherwise sound controls.”

This widens the potential impact, as theft of installed cabling or components can disrupt critical operations and damage assets.

For operators, terminals and cargo interests, this broader exposure means that the decision is not solely about protecting a load in motion. It is about protecting a strategically sensitive commodity across multiple handover points, including controlled sites and temporary storage. Vigilance therefore needs to extend from cargo security measures to site protection, monitoring, and risk awareness, to mitigate both direct loss and downstream interruption.

How criminals are gaining access

Loss severity has escalated alongside frequency. The data notes an even sharper rise in claim values, with 2025 representing a twenty-five fold increase relative to 2016 statistics. Higher commodity values contribute, but severity can also increase through larger load sizes, coordinated multi-vehicle events, and deception tactics that reduce the likelihood of early detection.

The methods used to access copper cargoes are evolving. Traditional hijacking remains prominent in certain regions, while deception-based theft represents an increasing proportion of cargo losses. Copper hijacking losses are heavily concentrated in Mexico through 2025, alongside increased fraudulent-carrier incidents in the USA.

This combination of physical theft and fraud-enabled collection reinforces a key operational point; copper theft is not only a physical security issue. It is also an identity, process, and authentication risk, particularly where subcontracting chains are complex and communications are fragmented.

How to reduce exposure

Effective mitigation is typically achieved through layered controls that address both physical and deception risks. The recommendations can be grouped into due diligence, fraud controls, operational discipline, and monitoring, with emphasis on consistency, particularly at handover points.

First, strengthening subcontractor integrity checks is fundamental. Enhanced due diligence is recommended, including verifying legal identity, physical office locations, operator licence details, company registration data, and director identities. Caution should be exercised where entities are newly formed or recently purchased, as such entities are disproportionately used as fronts for organised theft.

Second, deception and cyber-enabled fraud require specific countermeasures. Email verification software, avoiding free-domain email accounts, and requiring voice verification or multi-channel authentication for collection instructions are all prudent strategies. The operational aim is to prevent load release or diversion based on single-channel digital instructions that may be spoofed or compromised.



Third, journey planning and route controls should reflect copper's elevated risk. The use of pre-approved rest points with secure parking, no-stop rules during critical early movement phases, and avoidance of delivery areas known for criminal activity. Early arrival protocols should be defined to prevent drivers waiting outside unsecured facilities.

Fourth, equipment and technology should match the threat. Copper loads are recommended to travel in hard-sided, enclosed trailers, supported by multiple covert Global Positioning System (GPS) trackers embedded in both the unit and within the cargo. The draft notes that trackers should ping at variable intervals to reduce detection risk, and that constant 24/7 monitoring is essential, either internally or via contracted control rooms.

Finally, controlled handovers remain a high-leverage intervention point. Confirming driver identity in advance, sharing photographs and licence details with collection sites, and ensuring escalation processes exist if an unfamiliar driver appears are critical processes. Where risk is elevated, including in known hotspots or following clusters of incidents, escorts or shadowing vehicles could be considered, alongside ensuring cargo insurance arrangements appropriately reflect the risk profile of metals cargoes.

Pitfalls to avoid

Several recurring weaknesses can undermine otherwise sound controls. Over-reliance on digital instructions without multi-channel verification can enable fraudulent collection. Inconsistent onboarding across subcontractors can create a lowest-common-denominator standard in the chain, which is then exploited by reincarnated carriers. Journey planning that allows uncontrolled dwell time, particularly early in a trip or outside unsecured facilities, can also increase exposure.

Ports, terminals, and warehouses should also avoid treating copper as a standard commodity simply because it is common. The draft evidence suggests copper is frequently targeted, and risk controls should reflect that elevated profile, including consistent identity checks, documented handover protocols, and monitoring practices that are maintained even when operational pressure increases.

Conclusion

TT Club's 2016–2025 claims trajectory reflects a clear risk signal, copper theft is becoming more frequent, more costly, and more sophisticated. The trend is linked to market dynamics and amplified by process weaknesses in verification, subcontracting, and handover control.

A disciplined, layered approach combining robust due diligence, strengthened authentication, structured journey controls, and technology-enabled monitoring can materially reduce exposure. Applied consistently across transport, storage, and operational sites, these measures improve resilience when market conditions intensify criminal incentive.



Mike Yarwood
Managing Director Loss Prevention,
TT Club, London

Mike Yarwood is a Chartered Fellow of the Institute of Logistics and Transport, a Technical Specialist Member of the Institute of Risk Management and a Member of the Chartered Insurance Institute.

Trailer theft at a secure port facility

A 2026 cargo theft involving a high-value metal shipment moving from the United Kingdom to Germany provides a clear illustration of how organised criminals can exploit procedural weaknesses within a controlled logistics environment. The loss occurred during a multimodal movement via a UK port and a port in the Netherlands, and resulted in the disappearance of both trailer and cargo with an estimated value in excess of €100,000.

The case is notable not simply because of the theft itself, but because of the manner in which it occurred within a secured port facility, raising significant questions about insider involvement, information security and tracking reliability.

Context and sequence of events

The shipment comprised nickel, cobalt and molybdenum, transported initially by road from the north of the country to a port on the east coast before onward ferry movement to the Netherlands. Upon arrival, the trailer was placed within a closed and access-controlled terminal environment, where collection required presentation of a trailer unit code, booking number and driver identification.

Following the creation of a T1 transit document, the trailer was released from the terminal. However, subsequent investigation confirmed that the collecting vehicle was not associated with the contracted carrier. The trailer was actually collected on that day by a tractor unit bearing a Bulgarian licence plate, and the driver presented a Dutch identity card. CCTV at the port reportedly captured the vehicle and the driver, and the truck as it exited the premises.

The authorised driver arrived to collect the consignment but found that the trailer had already been removed. From that point, the cargo could not be located, and a formal theft report was filed with local authorities.

Evidence of insider-enabled theft

While the physical act of theft involved an unknown vehicle and driver, the circumstances strongly indicate that the crime was facilitated through insider knowledge. The individuals responsible were able to present the correct trailer unit code, booking references and access credentials required to satisfy terminal release protocols. This level of detail is unlikely to have been obtained through casual observation or external reconnaissance alone.

In practice, such incidents typically involve either direct insider participation or the leakage of operational information through compromised systems, personnel or communications. The criminals demonstrated precise awareness of timing, documentation status and collection procedures, including the creation of the transit document that triggered release eligibility. This suggests that sensitive shipment data had been accessed or shared in advance.

Tracking failure and likely GPS manipulation

The trailer was reportedly equipped with GPS tracking; however, the system proved ineffective in supporting recovery. Records indicate that the tracker intermittently reported the trailer as still being within the terminal in the Netherlands, despite the physical removal of the unit.

This behaviour strongly suggests that the tracking device was either discovered and deliberately interfered with, or that its signal

was manipulated. Two plausible scenarios arise. The device may have been located using radio frequency detection or scanning equipment and then removed and concealed on the terminal premises, thereby creating a false stationary signal. Alternatively, the signal may have been spoofed, allowing a false positional feed to be maintained while the trailer was removed.

Both possibilities highlight a growing vulnerability in high-value cargo movements. Criminal groups are increasingly capable of identifying and neutralising tracking systems within a short timeframe, rendering traditional GPS monitoring insufficient as a standalone security measure.

Risks and operational weaknesses

The incident demonstrates that secure infrastructure does not eliminate risk where procedural controls can be bypassed or exploited. Terminal access requirements were in place, yet these relied on data inputs that were evidently compromised. In parallel, the associated documentation process showed inconsistencies relating to invoices, weights and transit arrangements, creating an environment of administrative uncertainty.

Such conditions can reduce the ability of operators to identify anomalies in real time. When multiple parties are exchanging evolving shipment data across jurisdictions, the clarity needed to challenge an unauthorised collection may be diminished.

Implications for best practice

This case reinforces the need for more robust release verification processes at port and terminal interfaces. Authentication mechanisms should extend beyond static data points such as booking numbers or trailer identifiers, incorporating dynamic controls and cross-validation between systems and operational teams.

In addition, reliance on single-layer tracking solutions should be avoided for high-value cargo. Multi-layered monitoring, incorporating tamper alerts, geofencing and independent verification channels, may improve resilience against deliberate interference.

Finally, strict control of shipment information is essential. The protection of booking data, document status and collection timing should be treated as a core security function rather than an administrative process.

Conclusion

The theft of this trailer illustrates a shift in cargo crime towards intelligence-led methods. The combination of insider-enabled knowledge, effective impersonation at a secure facility and probable tracking manipulation demonstrates a sophisticated approach that can defeat conventional safeguards.

For operators and insurers, the lesson is clear. Physical security measures remain important, but equal attention must be given to information security, verification processes and the resilience of tracking technologies.

“

This case reinforces the need for more robust release verification processes at port and terminal interfaces.

”



Shifting carrier identities: a persistent threat to logistics integrity

Within the logistics sector, the issue of “reincarnated carriers” has become a significant concern, undermining the safety, reliability, and financial stability of supply chains. A reincarnated carrier is a transport company that, after accumulating a record of safety violations, enforcement actions, or unpaid penalties, deliberately shuts down and re-emerges under a new identity. This practice enables such companies to evade regulatory scrutiny and continue operations, often with the same personnel, equipment, and operational methods.

How reincarnated carriers operate

Reincarnated carriers typically operate multiple Motor Carrier (MC) numbers, running under the same dispatch and negotiating with the same brokers and shippers. Although they appear as distinct entities, they are frequently controlled by a single group. This deception is facilitated by the high demand for freight movement and the lack of robust vetting mechanisms, which can lead brokers and shippers to overlook warning signs.

The process is alarmingly straightforward. When a carrier's reputation is damaged – whether due to double brokering, theft, or safety concerns – the company is dissolved and reincarnated under a new name. Regulatory authorities such as the Federal Motor Carrier Safety Administration (FMCSA) have the power to consolidate records and issue out-of-service orders when patterns of noncompliance are detected. However, the sheer volume of applications and the sophistication of these operators mean that many evade detection.

Double brokering and cargo theft

Double brokering is a closely related issue, where a carrier accepts a load and then reassigns it to another operator without the shipper's knowledge or consent. This practice, often illegal, creates confusion over liability, insurance, and payment, and is a favoured tactic among reincarnated carriers. In recent years, the logistics industry has seen a rise in cases where carriers have held freight hostage, demanding ransom payments for its release. For example, in Illinois, dozens of loads were held for ransom, with total losses estimated at nearly \$5 million. Such incidents highlight vulnerabilities in carrier vetting processes and the need for greater transparency.

Safety and regulatory concerns

Reincarnated carriers are statistically more likely to be involved in severe crashes than compliant operators. Studies by the U.S. Government Accountability Office have found that these carriers are three times more likely to be involved in serious accidents. The risks extend beyond physical safety; insurers and brokers face complications in liability, subrogation, and claims recovery, particularly when ownership and address continuity are obscured.

Regulatory bodies have recognised the gravity of the issue, proposing new registration systems and risk-based vetting methodologies to identify and shut down reincarnated carriers. These initiatives aim to leverage data analysis, scrutinising registration patterns, shared addresses, and equipment modifications to assign risk scores and prioritise enforcement actions.

The European perspective

While reincarnated carriers are a global issue, they are particularly prominent in the European Union due to the lack of standardised regulations and the ease of cross-border transport. The EU's driver shortage and regulatory inconsistencies create fertile ground for

these operators, who exploit the system to move high-value goods with minimal oversight. The sophistication of their tactics – such as manipulating trailer seals, copying wrapping methods, and removing only a few units from loads to avoid detection – demonstrates a level of coordination that goes beyond opportunistic theft.

Mitigation and prevention

Addressing the threat of shifting carrier identities requires a multi-faceted approach. Rigorous due diligence, robust supply chain visibility, and thorough vetting of carriers are essential. Shippers must verify the identity of drivers and equipment at every stage of the delivery process, investigate discrepancies promptly, and report suspicious behaviour to authorities. Payment of ransoms should be avoided, as it only incentivises further criminal activity.

Industry collaboration is also vital. Sharing information on fraudulent carriers, leveraging onboarding platforms, and utilising carrier vetting tools can help identify and exclude bad actors from the supply chain. Regulatory bodies must continue to refine their detection methodologies, ensuring that reincarnated carriers are identified and removed before they can cause harm.

Conclusion

Reincarnated carriers represent a significant and persistent threat to the integrity of the logistics sector. Their ability to evade detection, exploit regulatory loopholes, and perpetrate fraud undermines trust and safety across the supply chain. Through enhanced vetting, industry collaboration, and regulatory reform, stakeholders can build resilience against these deceptive practices, safeguarding the movement of goods and the reputation of legitimate operators.



Josh Finch
Logistics Risk Manager

Josh is a Logistics Risk Manager for TT Club's Loss Prevention department. Josh joined TT Club in 2023 having 15 years of experience in the logistics industry in various operational and project management roles. He has extensive experience managing warehouses and running road freight transport operations. He is an International CPC qualified Transport Manager.

Existing Features Enhanced:	SAFER PARKING: IMPROVED TOOLS FOR IDENTIFYING SECURE TRUCK STOPS	DRIVER FEEDBACK: ALLOW DRIVERS TO LEAVE COMMENTS AND OPINIONS ABOUT TRUCK STOPS, VISIBLE TO HAULIERS.	ISSUE UPVOTING: FEATURE FOR USERS TO HIGHLIGHT AND UPVOTE CRITICAL ISSUES AT SPECIFIC TRUCK STOPS.
New Features:	FREIGHT CRIME REPORTING: REAL-TIME FREIGHT CRIME REPORTING DIRECTLY FROM DRIVERS AND HAULAGE COMPANIES.	MENTAL HEALTH & WELL-BEING SUPPORT HEALTHY EATING TIPS FOR DRIVERS VIA CV DRIVER ENHANCED FOCUS ON DRIVER MENTAL HEALTH AND OVERALL WELL-BEING.	COMMUNITY ENGAGEMENT: INDUSTRY-WIDE COLLABORATION TO RAISE AWARENESS ABOUT PARKING SECURITY AND WORKING CONDITIONS.
VISION:	INDUSTRY BENEFITS: ENSURES ALL STAKEHOLDERS - DRIVERS HAULIERS, AND THE LOGISTICS INDUSTRY - GAIN VALUE FROM THE APP.	SUPPORT FOR SECURE PARKING CAMPAIGNS: BUILDS ON EXISTING ADVOCACY EFFORTS FOR SAFER PARKING AND BETTER WORKING CONDITIONS FOR DRIVERS.	 MOTORWAY BUDDY

Help prevent cargo crime

NaVCIS Freight | Membership

NaVCIS Freight members receive:

- 26 fortnightly bulletins
- 12 monthly reports
- Four quarterly reports
- Our annual freight crime bulletin

Annual fees* based on size of your organisation:

- Small business £700 + VAT
- Medium business £2,500 + VAT
- Large business £4,500 + VAT

*Size of organisation determined according to published annual revenue. Fees correct as of September 2021. NaVCIS hopes to reduce the cost of fees in the future, as membership numbers increase.

For further details, contact us: freight@navcis.pnn.police.uk | 07388 859423



NATIONAL VEHICLE CRIME INTELLIGENCE SERVICE

navcis.police.uk | @NaVCIS_UK

