TT

TT Club Loss Prevention

November 2023

Supply chain security bulletin

What's inside?

Port and terminal security
A bold move: revolutionising transport access and security
Carrier fraud
Miami Dade Cargo Theft Symposium 2023

Contents

TT

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 providing an invaluable insight into the current risks facing those tasked with managing security through the supply chain. The Club has produced a number of reports and guidance documents related to this area of risk across numerous media platforms.

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

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

Foreword

Supply chain security remains a topic of concern globally. In particular there has been an uptick in claims incidence in North America, particularly involving fraudulent pick up, where the cargo is collected from the shipper by fraudsters. The loss prevention function continue to work with industry bodies, law enforcement and consultancy organisations to develop understanding and guidance for the Membership.

Pleasingly there has been a greater level of recognition given to these crimes by authorities in the last months. An existing relationship with and sponsorship of NaVCIS Freight in the UK recently led to an opportunity to profile the extent and societal impact of freight crime in the UK at an All Party Parliamentary Group meeting in Westminster. MP Greg Smith moderated the meeting that was attended by a variety of stakeholders from the industry, law enforcement, insurers and innovative solution providers. As a result of the meeting, the following day MP Greg Smith addressed the House of Commons challenging MP's to act to mitigate the associated risks. Pleasingly, it appears that the topic of freight crime is gaining further momentum at government level in the UK which in turn will assist in influencing greater industry engagement, particularly around safe and secure truck stop facilities.

The loss prevention function hosted an industry meeting in August where the Department for Transport (DfT) attended and presented about their role in influencing the standards (safety and security) of truck stop areas in the UK. The DfT highlighted a particular initiative involving a multi-million pound matched funding project for truck stop operators to make improvements to existing facilities.

Solution profile – Mobile Strongroom

Cargo theft, along with storage theft, is an escalating problem in the transportation and shipping industry, posing significant risks not only to inter-company supply chains but ultimately to the economy at large. Cargo theft has mushroomed into a multi-billion-dollar criminal enterprise, resulting in substantial financial losses for all parties involved, underscoring the urgency to address these vulnerabilities.

Here, Micaël Nyström, Founder and Managing Director of Mobile Strongroom, explains how his patented and certified innovative solution, addresses the challenge of cargo theft:

Mobile Strongroom is the only certified break-in proof intelligent vault shipping container in the world. It provides the highest level of container security for secure storage and safe transportation across ocean, road, and rail freight. It has fully reinforced protection for every elevation of the unit including the doors without a significant increase in weight and little compromise in space, due to our patented internal structure. Our smart vault comes equipped with an advanced real-time monitoring system to collect a wide variety of data.

Mobile Strongroom is tested by the independent state-owned research institute RI.SE and certified by SBSC in accordance with EN 1143-1 Grade 3, Scheme 5 (ISO/IEC 17067:2013). It is approved for storage of cash, explosives and weapons.

Key Features

- Keyless entry
- Self-locking
- Real-Time Asset Intelligence – Terminal
- Identifying & programable vault-lock system
- Third-party hardware/software integration ready, ie. mobile access
- High protection multi-lock, ballistic, blast and fire resistance

The Mobile Strongroom marks a significant advancement in the ongoing effort to protect global trade and supply chains from criminal activity. Mobile Strongroom is not just a secure container; it's a commitment to drive the shift towards a more secure, efficient, and sustainable transport industry.

| Theft-proof | Increase productivity | Lower costs | Reduce climate impact |
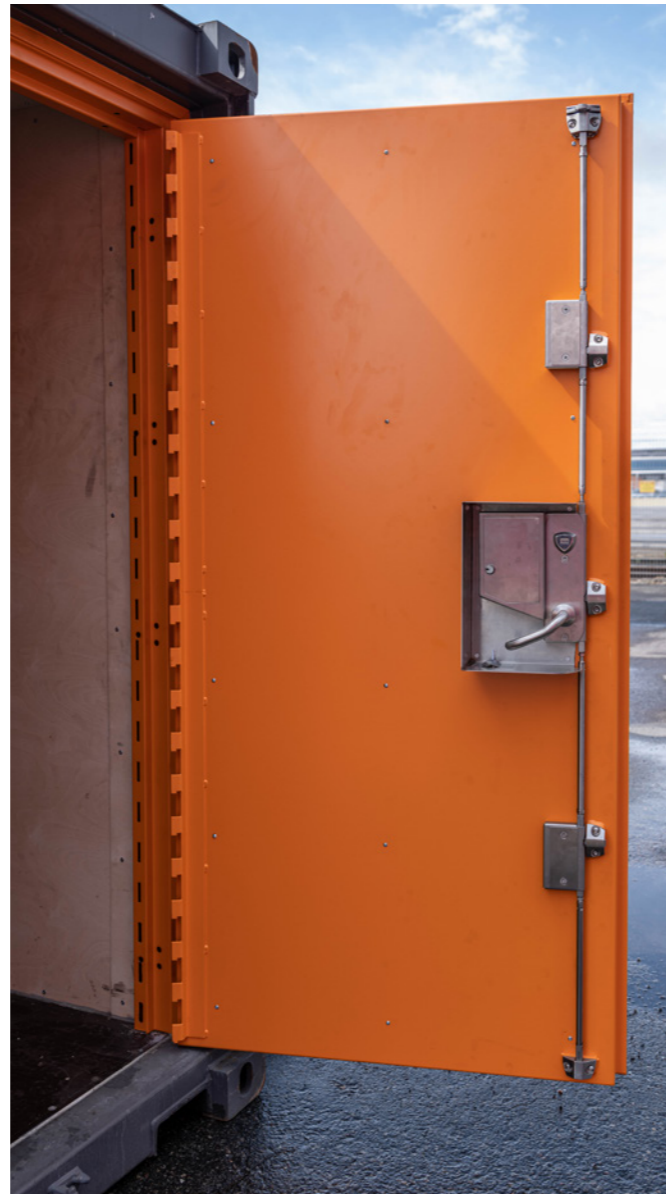
To find out more about Mobile Strongroom, visit www.mobilestrongroom.com, or email info@fmgss.com

Micaël Nyström
Founder, Mobile Strongroom

Micaël Nyström initiated the development of Mobile Strongroom in 2019. Coming from a background in the defense industry, Nyström recently served as the Sales Director at Saab, Business Area Surveillance, Airborne Surveillance Systems.

Mobile Strongroom

"The only certified vault shipping container in the world."

Port and terminal security

Security is key for container terminals and ports generally. The threat horizon is vast, incorporating cargo theft, illicit trades, alongside operational safety and the prevention of terrorist attacks. Inevitably, account is needed of both land and water interfaces.

A primary consideration in the context of security for port operators is the International Ship and Port Facility Security (ISPS) Code, a supplement to the Safety of Life at Sea (SOLAS) Convention considering maritime security, setting minimum security arrangements for ships, ports and government agencies.

Dating back to 2004, the ISPS Code ascribes responsibilities to a variety of stakeholders including port personnel, related to detecting threats and taking preventive measures affecting ships or port facilities used in international trade. The code specifies the appointment of a Port Facility Security Officer (PFSO), responsible for the development and maintenance of a Port Facility Security Plan (PFSP).

Barrier fundamentals

Physical security will be a primary consideration. Getting the simple things right, such as perimeter fencing is fundamental. Beyond that will need to be proportionate to the risks assessed, inevitably influenced by volumes, throughput, the type of cargo being handled, the layout of the terminal and the technology available.

There is an array of options and combinations to consider for perimeter fences; some designs may be more secure than others. It is recommended that palisade style fencing, for instance, be avoided as it may be more easily manipulated allowing access. A mesh style of fencing is generally thought to offer greater levels of security. The height of the perimeter fence is another critical factor, influenced by the local topography. A minimum two meter height is recommended to deter bad actors from scaling or being able to pass items over. Higher fences or topping with electric fencing or razor wire for added security may need to be considered.

Accessibility

Controlling access is a necessary starting point; strict access controls will assist in managing the flow of people, legitimate and otherwise to the facility. Thus, reduce the number of physical entry and exit points to the minimum necessary. Alongside this, consider how such areas will be monitored and managed. This includes the extent to which security personnel will be deployed, introduction of physical barriers, and what logs will be kept and for how long.

There will typically be a large number of restricted areas, buildings and rooms within a facility, where locks are utilised to prevent unauthorised access. Regardless of who may have them, robust processes are necessary to ensure that keys are returned and controlled, with timely intervention protocols.

Key control and operational efficiencies may be significantly improved by the implementation of electromechanical key systems; these remove the risk of lost or stolen keys and security compromises, while providing valuable user data for management and control. Central programming ensures efficient and speedy modification of access permissions. Further smart and high security locks may be appropriate.

Line of sight

The deployment of cameras can add to security provisions and can have dual benefits. Sophisticated camera systems monitoring the entry gate can serve not only to record access, but also capture the condition of the vehicle, container, chassis and cargo. All such records might prove invaluable evidence in the event of any dispute.

Cameras can also be linked to the Terminal Operator System (TOS) and, using Optical Character Recognition (OCR) technology, can drive the development of operational efficiencies, identifying and locating individual containers. Automatic Number Plate Recognition (ANPR) cameras can identify expected site visitors, providing both security and efficiency, potentially controlling the release of vehicles and containers with a binary "release, don't release" prerogative.

Visual analytics software can provide unrivalled insight, including managing the movement of visitors, restricting and controlling the areas of the facility that they are able to access. Additionally, if linked to the relevant authority and national databases, this could serve to identify bad actors and vehicles operating on false registration plates, often used to facilitate theft of cargo.

Thermal cameras are now being used for both security and fire detection. These may eliminate the need for continuous monitoring of cameras by alerting security personnel at the point of detection due to a fire or a person.

CCTV cameras and software can also provide a deterrent to bad actors. However, take care to ensure that the procured system is fit for purpose, well maintained and that operators are trained to use the equipment proficiently. And don't forget simple housekeeping – overgrown foliage or litter can trigger unwelcome false alarms.

Interfaces

Some facilities might fall under the jurisdiction of the port police; regardless, working closely with local law enforcement will be vitally important. While operation specific security measures should always be implemented, interacting with port police or other local law enforcement agencies will be beneficial in 'layering' protections.

Technology can provide advanced levels of security. Drones are a recent addition to the security managers' armoury – these may provide remote and autonomous surveillance, supplementing existing people and processes. Capable of deploying either to a set time period, randomly or in reaction to an alarm, security drones can capture valuable footage – and operating at height provides a barrier for intervention.

Technologies are likely to overcome the human, moral hazard. This can be further enhanced, for example with forensic coding security solutions – gels, sprays and liquids can be an effective deterrent, remaining on clothing and skin for prolonged periods, and thus increasing the risk of apprehension. This may be during questioning in relation to unconnected crimes, since those involved in criminal activity in and around ports will typically be involved in other crime.

> **Information is the lifeblood of criminal activity and can be sourced from within an operation.**

Information security

Insider risk is prevalent within TT's claims experience; information is the lifeblood of criminal activity and can be sourced from within an operation. This may be access codes, the location of a particular container or details of security provisions on site.

Information security is a critical. Carry out a risk assessment of the information that your operation collects, stores and shares. Recognise the value of that information in the wrong hands and consider thoroughly who has access and why, balancing access restrictions with operational efficiency. Prevent workstation sharing or sharing of passwords.

The terminal operating system (TOS) is pivotal in the management of the container terminal. Protecting this key infrastructure is critical to maintain operational integrity and avoid business disruption.

Peregrine started with the TT Club in 1984, handling claims and providing advice to all types of transport and logistics operators, including ports and terminals. Since 2002, Peregrine has led the TT's Loss Prevention function, being involved in a broad range of safety and security issues facing the industry, particularly interfacing with inter-governmental organisations and industry associations.

A bold move: revolutionising transport access and security

David Rock, Market Development Manager at Abloy UK, discusses the security and access challenges faced in the transport and logistics sector, exploring new digital access solutions that improve operational efficiency and security with reduced costs, logistics and risk of lost keys.

Effective access control and security in the transport and logistics sector is vital, with ongoing threats from cargo theft, misuse of vehicles, and malicious attack. High-value assets in this industry range from trucks, ships, aeroplanes and rolling stock, to containers holding high value goods, all of which need to be protected.

Although the 2022 Cargo Theft Report[1] from TT CLUB, TAPA EMEA and BSI Connect SCREEN Intelligence recorded fewer cargo theft incidents globally in 2022 compared with previous years, vigilance is still paramount.

There has been a steady increase in criminals targeting basic goods such as food and beverages, automotive and truck parts, and fuel, and a sustained theft of higher-valued goods like electronics. The report suggests this is in large part due to the macro-economic impact of inflation, or the loss of purchasing power on criminal patterns.

Ports, airports, railway stations and transport depots are ideal environments for criminals - their size, numerous entry and exit points, and the volume of people flowing through them makes it easy for illegal activity to occur undetected.

Consistent surveillance is required, and a vast perimeter and 24/7 operations mean the sheer scale of the necessary security is immense. Plus, any security and access provisions need to not impede or slow down processes in any way. Cargo theft is common, with unattended containers providing an ideal target for both opportunistic and organised criminals.

All these contributing factors make for a challenging environment in which to secure access. With a range of additional potential threats to consider too, such as people trafficking, drug smuggling and terrorism, maintaining a secure environment and controlling access can seem insurmountable.
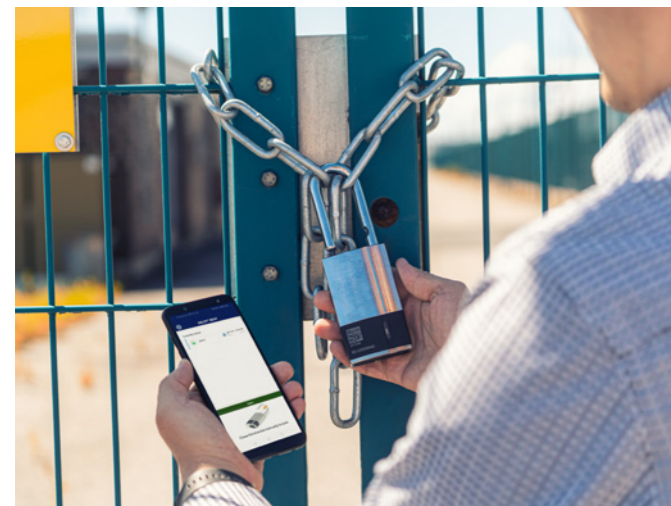
Issues relating to security can cause long-term damage to a company's credibility. Most businesses in the sector need to deliver services 24/7, and any interruption to this service can result in loss of revenue and a tarnished reputation.

The current economic and political environment does not help to reduce potential risks, so mitigating potential vulnerabilities, such as a breach in health and safety, while at the same time improving efficiency and traceability must be included in the daily management routines to protect assets.

Meeting security requirements

Security requirements vary between different organisations, but the need for high security solutions is universal. Vehicles and the areas in which they are kept when not in use need to be secured, but also accessible at all times for business to run effectively.

Vehicle and container security begins with effective physical security devices including locks. Key control, traceability of key use and up-to-date, accurate access rights are vital.

In ports environments, there are currently no specific locking standards that regulate security, access control or processes, unlike in other industries that are highly regulated.

Many mechanical keys are required to access estates and property, warehouses, perimeter gates, passenger terminals, engineering control rooms, high-voltage areas, cranes and other locations. Using mechanical locks has traditionally proven to be a good investment, forming part of a layered security approach. However, as security and access control technology has evolved, these solutions have become outdated, with numerous limitations.

Manual essential control can be complicated and time-consuming. Adding new keys or scaling up legacy systems with mechanical technology can add to the complexity of managing security and access control.

Abloy's solution

With this in mind, Abloy offers a portfolio of access solutions to not only future-proof security for transport and logistics environments, but also add extra operational efficiency. This includes a range of keyless, electromechanical and mechanical solutions, such as container locks, to secure the entire infrastructure.

Abloy solutions go beyond high-end security and access control, enabling remote access control and simplified key management with precise audit trails. Mechanical solutions are robust and offer high strength and durability, designed to operate in harsh environments.

PROTEC² CLIQ® and ABLOY® BEAT lead digital transformation and operational efficiency within critical infrastructure. They enable

1 https://www.ttclub.com/media/files/tt-club/bsi-tt-club-cargo-theft-report/2022-tt-club-tapa-emea-and-bsi-annual-cargo-theft-report-1.pdf

> **Abloy offers a portfolio of access solutions to not only future-proof security for transport and logistics environments, but also add extra operational efficiency…**

remote locking, essential control, and management on the go, adding a new level of operational efficiency.

PROTEC² CLIQ® is also well suited for transport environments where mobile phone use is restricted. The pre-programmable electromechanical keys provide the convenience of remote control and high security throughout the business, anytime, anywhere.

ABLOY® BEAT is a new digital locking solution that includes a Super Weatherproof Bluetooth padlock operated with a digital mobile key and secured with the best-in-class Seos® credential technology.

Both PROTEC² CLIQ® and ABLOY® BEAT can be managed with ABLOY CIPE.

CIPE Manager provides digital convenience, control and security that simplifies managing an operation while adding operational efficiency and complete situational awareness.

CIPE Manager allows for keys, locks and access rights to be managed on the go with a user-friendly visual mapping cloud-based management system. It connects with Abloy's digital portfolio, including ABLOY BEAT, PROTEC² CLIQ, and ABLOY mechanical master key systems.

Abloy padlocks achieve the highest security grade of BS EN 12320:2001 accompanied with the highest grade of corrosion resistance. Our IP68 rated padlocks also have certification LPS 1654 Issue 1 SR Level 1-4 and carry the "+" rating against surreptitious manipulation from the Loss Prevention Council Board (LPCB).

Abloy has a proven track record of helping to protect critical infrastructure for over half a century and is committed to providing the best security solutions advice and support to help safeguard resilient and continuous services.

ABLOY

For further information on products and services available from Abloy, visit https://bit.ly/3KeP7aB, call 01902 364 500, or email info@abloy.co.uk.

David Rock is a member of the Abloy UK Critical Infrastructure team, specialising in addressing the security and access management challenges faced across the transport sector – particularly ports, airports and highways.

Carrier fraud

TT have witnessed a significant uptick in the frequency of cargo theft incidents in North America through 2023. In many instances fraudulent strategies employed by the criminals have afforded opportunity to gain access to their target cargoes. Here George Radu, Claims Executive based in TT's San Francisco office explains how the frauds work and provides loss prevention guidance to mitigate the risks.

The strategy illustrated in this article is increasingly being used by cargo thieves in North America, it would be prudent for all transport operator Members to be aware.

A company providing logistics services out of Texas arranged for a collection of high value cargo for their customer, which they arranged to be transported using subcontracted hauliers to a buyer in Illinois. A truck driver duly arrived and collected the goods from the shipper, unfortunately, the cargo never made it to its destination.

As soon as the cargo departed the warehouse, the driver cut off all communication. Attempts were made to contact the subcontractor company using the contact details provided but the attempts were unsuccessful. Two days after the cargo disappeared, the thieves made contact, stating that the load had been stolen and transported across the international border into Mexico.

The thieves knew the value of the cargo and, in a scheme reminiscent of recent online ransomware attacks, they demanded that a percentage of the value of the cargo be paid into a bank account to be provided in exchange for moving the stock back across the border to an undisclosed location in Texas. They gave a very short deadline with a view to hurrying the logistics provider into a decision in their favor, stating that a failure to act would result in sale of the stock on the Mexican black market.

The Logistics provider searched for the hauliers businesses using a registry monitoring service and contacted them using details they found online. They were informed that the thieves had stolen the identities of these legitimate businesses. Unfortunately, this knowledge came too late to prevent the theft of $245,000 worth of cargo.

Practical loss prevention guidance

The ingenuity of cargo thieves should not be underestimated, it is becoming ever more difficult to detect fraudulent activity as criminals seek to employ counter measures in place to avoid detection. Robust due diligence procedures as a component of a layered security approach will provide greater security. There are also a number of practical operational strategies that could be employed by logistics operators as set out below:

1. Where practicable, only use trusted haulage providers. Avoid arranging transport with unknown entities via freight exchanges.

2. Confirm all information provided by the potential carrier is correct: We know perpetrators use different phone, fax and emails than the actual carrier. Consider using security platforms such as Carrier411, or perform a quick internet search on the carrier's name. Numerous websites should provide the actual contact and equipment details for the actual trucker. If the contact details are different than those provided, a red flag should be raised and proceed with caution.

3. Once identified, contact the real trucker through a known phone number from your searches. Confirm the following with the real trucker:

   a. Company name, name of owner/driver, address, phone and email

   b. Size of operation, number of drivers and pieces/type of equipment

   c. Area of coverage; interstate or intrastate, Canada

   d. When did you submit your carrier information to book a move?

4. Once it has been established that you are talking with the real carrier:

   a. Confirm name of driver assigned to pick up the load

   b. Confirm signage and license plate information on tractor/trailer and provide the same information to the shipper for further confirmation at the time of pick up

   c. Where ever possible refrain from asking questions that will result in "yes" or "no" answers. Instead, ask the line of questioning listed above since you should be speaking to the real carrier.

Below is a non-exhaustive list of recommendations that should be carried out by the warehouse or cargo releasing facility:

1. Take a photocopy of carrier's Commercial Driver's License

2. Confirm carrier's driver's license is a valid

3. Place a video or CCTV camera on the back wall shipping offices facing the driver window for clear identification of the collecting driver

4. Take a right thumbprint of unknown/unexpected drivers

5. Require drivers to sign in when arriving at the shipping window and verify their information on the sign in sheet. Ask the driver to wait while the their identity is verified with the trucking company

6. Photograph and confirm signage, numbers and plates on tractor doors and trailer. If signage does not match carrier's information provided by the transportation broker or the signage is covered and not visible, contact the transportation broker for clarification and/or further instruction.

George Radu
Claims Executive

George Radu joined TMA in 2007 after spending 19 years at a major container shipping line including 10 years as Claims Manager. He handles cargo related claims and is the America's Loss Prevention officer.

> "Take time to consider risks – if something seems too good to be true – it probably is."

> ❝ **The United States is experiencing a 10-year high in cargo theft, with no signs of slowing down.** ❞

Miami Dade Cargo Theft Symposium 2023

In September, partly in recognition of a spike in cargo theft incidents in North America, Guillermo Cancio, Senior Claims Executive based in New Jersey travelled to and attended the annual Miami Dade Cargo Theft Symposium.

Miami Dade County Police (MDPD) hosts the Miami Dade Cargo Theft Symposium to allow professionals to network and to encourage knowledge transfer from the department's experienced cargo theft detective unit to other police departments and the supply chain industry at large. The 2023 conference was attended by law enforcement representatives from the US Department of Homeland Security, including US Customs, private investigators, insurance representatives, security vendors, cargo surveyors, and property brokers. Speakers highlighted the exponential growth of "strategic theft" and the unprecedented costs incurred to be incurred by the industry, especially brokers. All speakers emphasized the industry's need to collaborate to disrupt thieves.

The United States is experiencing a 10-year high in cargo theft, with no signs of slowing down. The average value of losses increased to $265,000.00 in 2022. Although cargo theft continues to be concentrated in California, Florida, Texas, and Illinois, the incidence of cargo theft is spreading to other jurisdictions where these issues were previously unheard of. This coincides with the fact that there are fewer law enforcement officers dedicated to cargo theft than before 2020. Among the challenges faced by law enforcement in the investigation of cargo theft is the seemingly simple question of incident reporting.

The importance of reporting

Many times, when receiving a notice of cargo theft, law enforcement officers decline to action reporting a cargo theft incident due to firstly, law enforcement's inability to become involved in contractual disputes (i.e., hostage loads) and secondly

the caller not appropriately conveying the details of the occurrence or three, the officer not understanding the information conveyed by the caller.

Attendees were cautioned that when reporting a cargo theft incident, a claimant should specify the following:

1 Incident involves cargo "moving in commerce,"

2 Taken by an unauthorized party,

3 With a bill of lading, or other transit document, to prove it,

4 With (or without GPS tracking); and

5 A contact available at all times to arrange for the recovery of the load.

Often, a caller does not have documentation available to help law enforcement, and as much documentation as possible should be made available contemporaneously with reporting the incident.

Guillermo Cancio is a Senior Claims Executive for Thomas Miller Americas based in New Jersey and handles TT Club Member claims. Guillermo has experience in a vast range of complex cases and sees first-hand the effects of these claims on individual businesses.

Fictitious pick up's affect all modes

The perils of fraudulent collections are felt far and wide through the entire global supply chain, the air mode being no exception. Operators within the air cargo supply chain have witnessed an uptick in theft activity in the last two years particularly where fraudsters present themselves to collect cargo from warehouse facilities with forged documentation.

CCS-UK was launched in 1993 and is the central core of a new-style community system that replaced ACP 90, which used a central Customs computer connected to dedicated terminals located in freight agents' offices, over dedicated data lines. CCS-UK more recently introduced "distributed processing" and, in doing so, created a real digital cargo community. This comprised air forwarding agents using their own PCs and specialist programs to send and receive messages via the CCS-UK central database and switch.

Central to the air freight community in the UK and recognising the challenges around theft and fraud that the stakeholders face, CCS-UK have developed a new e-collection note. Guy Thomas, Programme Director for the CCS-UK User Group at CCS-UK tells us more about this new initiative.

CCS-UK trials e-collection note

A new, electronic air cargo collection note is set to revolutionise cargo collections from airlines' ground handlers in the UK, improving security and efficiency.

Designed by CCS-UK as the latest enhancement to its Advance Information System (AIS), the "e-collection note" replaces the traditional paper version which has been in use for decades. The old paper-based system requires agents to produce a hard-copy collection note, which their own driver or transport contractor then presented to the handling agent in order to obtain release of the cargo.

Not only are current processes time-consuming, but there can be an increased risk of fraudulent activity.

The new, electronic version is downloaded as a QR code by the forwarder, direct to the driver's pre-registered smartphone. This is scanned when the driver arrives at the handling agent to collect the cargo which initiates a check against the shipment collection advice along with validation of driver and vehicle details.

If there is any discrepancy, the handler will not release the goods; however, in the event of a legitimate cause for the discrepancy (such as last-minute change of driver or vehicle), the process enables freight forwarders to amend the collection advice, avoiding the need for the driver to return to base.

Logistics service provider GEODIS and cargo handler Dnata are currently trialling the new system at London Heathrow airport. It is expected that the new process will significantly reduce the risk of fraudulent collections that have always existed with paper collection notes.

The e-collection note is a further enhancement of the CCS-UK AIS module, which enables freight agents and their transport contractors to pre-advise transit sheds of their air import collections and export drop-offs. Submitting this information via AIS enables handlers to better allocate their resources and schedule workflows. By pre-allocating truck door slots, they can reduce truck queues and waiting times during peak periods. Freight agents can also use the AIS 'Air waybill watch' feature to track specific air waybills and receive updates on the shipment status, enabling them to better plan vehicle movements.

AIS is free to all registered CCS-UK users.

> ❝ **A new, electronic air cargo collection note is set to revolutionise cargo collections from airlines' ground handlers in the UK.** ❞

Guy Thompson
Programme Director for the CCS-UK User Group

The User Group works alongside BT in the provision of the CCS-UK system. This system interfaces between and provides functionality to support the Freight Forwarders, Transit Sheds, Airlines and Customs and Border Force systems for air cargo imports and exports. The system operates for the majority of UK airports. The User Group responsibilities are the identification and definition of new and evolving requirements for the air cargo community and is comprised of directors from large companies that operate in the air cargo sector.

Previous position

Guy was the IT Director of Servisair, a major ground and cargo handling company that operated in 200+ airports, responsible for all IT systems and infrastructure.

Strategic Theft: A New Frontier

Although straight theft continues to be the most significant modus operandi of thieves, experts expect strategic theft to grow to become the most common form of cargo theft in the near future. Strategic theft is when criminals use fraudulent information in order to take possession of the cargo, for example, identity theft, fictitious pickups, cyber double brokering scams, etc. Experts at the at the recent Miami Dade Cargo Theft Symposium agreed that known advice to combat straight cargo theft in the supply chain also applies to strategic theft: proactive risk management to prevent and quickly identify incidents once they occur. However, unlike incidents of straight theft, shippers have the most opportunity to avoid cargo theft at pickup. Therefore, engaging customers about the threat of strategic theft and means of mitigating potential losses is critical.

Is #cargotheft #supplychainfraud awareness becoming mainstream?

Transportation and logistics professionals have long known about the ever-evolving threat to cargo in the supply chain. However, as incidences of organized retail crime, including cargo theft and supply chain fraud, have gone viral, so has the public's attention to cargo crime. An example of increased public interest was the introduction in early 2023 of the Combating Organized Retail Crime Act (S. 140/H.R. 895). Although the bills are still before their respective first committees, the US Chamber of Commerce and the National Retail Federation's support increases the likelihood of the act becoming before the end of the 118th session of Congress in December 2024.

In the month leading up to this article, the New York Times published a slick multimedia investigative piece detailing the theft of a load of highly sought-after candy while in domestic transit between California and New Jersey. To the layman, the article "How to Hijack a Quarter of a Million Dollars in Rare Japanese Kit Kats"[1] details a story familiar to industry insiders: a convoluted cat-and-mouse game where a freight broker faces claims from its customer for negligent brokering while the shipper appears to have contributed to the loss by failing to vet the motor carrier before releasing the cargo.

Lastly, in the day leading up to the drafting of this article the social media platform Barstool Sports published a Tik-Tok story liked over 350k times details the indictment of a college student for defrauding a supply chain supplier with fraudulent claims. The student gained access to the supplier's computer system and would approve returns and refunds to himself and

co-conspirators in excess of $3.5 million. While news about an indicted supply chain fraudster makes its way into industry publications or your LinkedIn feed; its inclusion in Barstool's TikTok video feed points to the mainstream awareness of cargo theft and supply chain fraud.

As the incidences of cargo theft and supply chain fraud continue to increase, the supply chain industry can expect increased awareness from the public at large and government officials. The increased awareness should be seen as an opportunity for the industry to leverage the awareness for improved resources to investigate and convict those responsible for these crimes.

> " Transportation and logistics professionals have long known about the ever-evolving threat to cargo in the supply chain. "

Guillermo Cancio is a Senior Claims Executive for Thomas Miller Americas based in New Jersey and handles TT Club Member claims. Guillermo has experience in a vast range of complex cases and sees first-hand the effects of these claims on individual businesses.

1 https://www.nytimes.com/2023/11/08/dining/kit-kats.html
2 https://www.tiktok.com/@barstoolsports/video/7303433149856386347