

**TAPA** EMEA  
Transported Asset Protection Association

# TAPA EMEA Driver Security Guide

TAPA EMEA Copyright © Do Not Copy



 ENGLISH

## Content

<b><u>INTRODUCTION AND SUPPLY CHAIN SECURITY ENVIRONMENT .....</u></b>	<b><u>3</u></b>
<b><u>COMMUNICATION WITH POLICE AND MANAGEMENT .....</u></b>	<b><u>4</u></b>
<b><u>TYPES OF CRIMINAL ACTIVITY .....</u></b>	<b><u>5</u></b>
<b><u>INTRUSION, ROBBERY &amp; THEFT .....</u></b>	<b><u>6</u></b>
<b><u>DECEPTION .....</u></b>	<b><u>8</u></b>
<b><u>HIJACKING .....</u></b>	<b><u>11</u></b>
<b><u>ILLEGAL IMMIGRANTS ENTRY .....</u></b>	<b><u>13</u></b>
<b><u>LAST-MILE VEHICLES CRIME .....</u></b>	<b><u>15</u></b>
<b><u>CYBERCRIME AND INFORMATION SECURITY LEAK .....</u></b>	<b><u>17</u></b>
<b><u>DISPATCHING OR MONITORING &amp; RESPONSE CENTRES FUNCTIONALITIES AND SUPPORT TO DRIVERS .....</u></b>	<b><u>19</u></b>
<b><u>EUROPEAN EMERGENCY CONTACT NUMBERS .....</u></b>	<b><u>21</u></b>
<b><u>DRIVERS' VALUABLE RULES .....</u></b>	<b><u>22</u></b>
<b><u>REFERENCES .....</u></b>	<b><u>23</u></b>
<b><u>DISCLAIMER FOR THE DRIVER SECURITY GUIDE .....</u></b>	<b><u>23</u></b>

THP  
APR  
MAY  
COPYRIGHT © Do Not Copy



# Communication with Police and Management

Effective communication with police authorities and carriers' management is crucial for drivers, especially during abnormal situations. In these unfortunate situations, drivers must communicate important information in a clear and accurate manner. Language barriers can be a challenge, as drivers may not speak the local language. In such cases, there are mechanisms provided by professional monitoring centres that can help by using native speakers to communicate with local authorities. Some of these monitoring centres have a network of centres and security companies along the drivers' routes to provide support in case of incidents, either by providing onsite security services if required or to facilitate local interaction with police and medical emergency services.

In case of a security incident, drivers must be able to communicate accurately at least the following information with the police:

- Name of driver and license plate of the vehicle (truck and trailer)
- Special characteristics of the vehicle (colour, brand, special logos, etc.) that shall facilitate the police forces to locate the vehicles
- Location of the vehicle (as accurately as possible) using either km marking of the road, or nearest city/village passed, or any landmark (i.e. service station, etc.)

- Type of incident and if medical support is needed.

Communication with carriers' management in case of an incident, should provide the same accuracy and a minimum set of information, focused mostly on the last two points above, as drivers' and vehicles' data are well known to the carriers.



# Types of Criminal Activity

In this In the Drivers' Security Guide, we will explore common types of criminal activities and provide tips on prevention, response, and reporting. According to the latest Europol report, there are 821 criminal networks in the EU with over 25,000 members. These networks engage in various crimes, including drug trafficking, fraud, property crime, migrant smuggling, and human trafficking. Drug trafficking is a prominent activity, with 50% of the most threatening criminal networks involved in it, and 36% solely focused on drug trafficking. We shall also analyze several specific types of criminal activities in a way to present only the topics that can be directly affected by the drivers and provide some guidance with easy to understand and remember drivers' actions that must be taken or avoided during such incidents. In most of the crime types analyzed, we have also included some related examples.

## MOST TARGETED PRODUCTS – TOP 5 COUNTRIES



### South Africa

1. Phones
2. Cash
3. Misc. Electronics
4. Metal
5. Food & Drink



### United Kingdom

1. Fuel
2. Food & Drink
3. Tobacco
4. Clothing & Footwear
5. No Load (Theft of truck and/or trailer)



### Germany

1. Fuel
2. Metal
3. Tools/Building Materials
4. Auto Parts
5. No Load (Theft of truck and/or trailer)



### France

1. Fuel
2. Metal
3. Jewellery/Precious Metals
4. Misc. Electronics
5. Food & Drink



### Sweden

1. Fuel
2. Metal
3. No Load (Theft of truck and/or trailer)
4. Cash
5. Food & Drink

**Note:** TAPA EMEA is recording losses in over 20 TIS product categories. However, across EMEA, most recorded cargo crimes stated the products targeted as unspecified or miscellaneous.

## Intrusion, Robbery & Theft

### What is Intrusion, Robbery & (Cargo/Fuel) Theft Threat?

There are several situations which criminals manage to enter the cargo compartment (intrusion) and partially steal cargo from it. There are also cases where the criminals manage to steal the whole truck or trailer with the full truck load.

### How to prevent Intrusion, Robbery & Theft Threat?

To reduce the risk of intrusion, robbery, or theft, it is advisable to stick to the planned route and avoid unscheduled stops or changes, as these unscheduled events offer to criminals the desired opportunity to attack. Although following the plan does not guarantee complete safety and security, it significantly decreases the likelihood of becoming a victim. Furthermore, it is recommended not to arrive too early at the destination facility, as waiting outside exposes both the driver and cargo to criminals who are active in logistic parks. Additionally, there has been a remarkable increase in reported incidents of fuel theft recently, involving both small and large quantities of diesel.

If you have already been affected or become a victim of an Incident/ robbery, please share the type, extent, location, and kind of products involved with us via the following email address: [tisteam@tapaemea.org](mailto:tisteam@tapaemea.org).

This way, we can record the incident in our TAPA EMEA database and help other drivers and dispatchers respond to relevant trends

#### THEFT FROM VEHICLE INCIDENT ON 12.03.2024

Incident Details	Place	Product
<b>DATE</b> 12.03.2024	<b>City</b> -	<b>CATEGORY</b> Miscellaneous Electronics
<b>INCIDENT CATEGORY</b> Theft from Vehicle	<b>REGION/ COUNTRY</b> -/ Germany	<b>PRODUCT DETAILS</b> Electrical appliances
<b>MODUS OPERANDI</b> Intrusion	<b>LOCATION TYPE</b> Unclassified Parking	<b>VALUE IN EUR</b> 150,000.00
	<b>LATITUDE/ LONGITUDE</b> 51.401352397921/ 11.719513675255	

Source: TIS database

#### THEFT FROM TRAILER INCIDENT IN 20.02.2024

Incident Details	Place	Product
<b>DATE</b> 20.02.2024	<b>City</b> Naples	<b>CATEGORY</b> Miscellaneous
<b>INCIDENT CATEGORY</b> Theft from Vehicle	<b>REGION/ COUNTRY</b> -/ Italy	<b>PRODUCT DETAILS</b> Perfumery and Tobacco products
<b>MODUS OPERANDI</b> Intrusion	<b>LOCATION TYPE</b> Unclassified Parking	<b>VALUE IN EUR</b> 2,400,000.00
	<b>LATITUDE/ LONGITUDE</b> 40.8517746/15.2681244	

Source: TIS database

## Secure Parking Areas

When taking breaks during your route, it is recommended to use secure parking areas. Consult with your dispatchers before starting your journey to locate these secure parking areas along your route. The advantages of using secure parking areas include:

- Enhanced safety and security for both the driver and the cargo, reducing the risk of criminal activity.
- Access to resting and hygiene facilities to help drivers relax during their breaks.
- In the event of an incident, security systems like CCTV can provide evidence to support police and internal investigations.

## Unscheduled Stops and Unplanned Change of Routes

Criminals often seek to exploit any irregularities in your route, as they view them as opportunities to attack you and steal the cargo. It is crucial to remain vigilant and minimize any unscheduled deviations or disruptions that could create such opportunities

## How to prevent Intrusion, Robbery & Theft Threat?

### DOs







- Protect yourself. If you are in your cabin, stay inside.
- Call the police immediately.
- If your truck is equipped with a panic button, press it, or try to communicate with your monitoring/dispatching centre.
- Gather as much information from the criminals to share with the police.
- Preserve the crime scene, to support investigation teams.
- If you must park outside a secure parking area:
  - Position the loading doors of your truck/trailer against a wall, building, or another trailer/vehicle.
  - Keep the stop/break as quick/short as possible.
- Use locking fuel caps and anti-siphoning devices to prevent fuel thefts.

### DONT'S

- DO NOT try to defend the cargo by confronting the criminals, as it can put your life at risk.
- DO NOT change your planned itinerary and scheduled stops, unless necessary, and inform your dispatching centre while taking additional security measures.
- DO NOT change your delivery address without positive confirmation from your dispatcher.
- DO NOT rely on passers-by to guide you if you are lost; it is better to ask them for information about your location instead.

## How to report Intrusion, Robbery & Theft Threat?

If you experience a security incident involving intrusion resulting in robbery or theft of your cargo, report as below or report the following information to police / monitoring centre and/or dispatching centre:

-  Time/date/location of the incident
-  Any injury or need for emergency health support
-  Name of driver / license plates of truck/trailer
-  Number of criminals involved
-  Criminals modus' operandi (how did it happen)
-  Estimated cargo loss

## Deception

### What is Deception Threat?

In many cases, attackers shall try to get access to the cargo not by forcibly attacking it but by side means. This modus operandi involves using deceptive means to trick brokers, carriers, shippers, and of course drivers to hand over a load to the thieves instead of a legitimate business. Thieves will impersonate legitimate shippers, brokers, police, or other authorities, even drivers to get the cargo. In some cases, attackers may target the security systems onboard the vehicles, attempting to confuse or misinform the driver about the cargo's location. They may also intercept or block communication between the driver, dispatching/monitoring centre, or police authorities. Intercepting on-vehicle sensors and devices is another tactic used by attackers against cargo transport operations.

Bogus drivers pickups are approximately 2% of total cargo thefts in Europe, but in some cases the losses are of significant value. In November 2023, a bogus driver impersonating the real one managed to steal mobile phones from Schiphol airport in Amsterdam, with a value of more than 1.5 million Euros.

### THEFT OF TRAILER INCIDENT ON 10.11.2023

Incident Details	Place	Product
DATE 10.11.2023	City Reims	CATEGORY Food & Drink
INCIDENT CATEGORY Theft of Trailer	REGION/COUNTRY -/France	PRODUCT DETAILS champagne
MODUS OPERANDI Deception Others	LOCATION TYPE En Route	VALUE IN EUR 600,000.00
	LATITUDE/ LONGITUDE 49.258329/ 4.031696	

Source: TIS database



## How to prevent Deception Threat?

- Prevent impersonation  
To prevent impersonation and potential fraudulent actions by criminals, it is important to remain cautious and follow these guidelines:
  - If you are stopped by someone claiming to be the police or another authority for a check, be vigilant and consider the possibility of impersonation.
  - If, just before arriving at the delivery facility, an employee of the warehouse informs you that you must deliver to a different location, always verify the information with your dispatching centre before proceeding.
- **Avoid Jamming and Spoofing**  
Jamming refers to intentionally blocking communication signals, rendering devices unable to transmit or receive any form of communication (voice calls, SMS, alarm signals, etc.). Spoofing, on the other hand, involves fraudsters using deceptive techniques to gain victims' trust by altering caller IDs or sending messages that appear to be from a different source, trustworthy by the drivers.

**On 16 May 2023, cargo thieves attacked and hijacked a truck travelling en route from Port Elizabeth to Cape Town, South Africa. The truck driver was shot and seriously injured.**

After taking control of the vehicle, the offenders used a GPS jammer to delay security monitoring services and drove the vehicle to a remote location to offload and steal its cargo.

The target: catalytic converters.

This is just the latest in a series of high value and violent attacks on automotive supply chains in the Europe, Middle East & Africa (EMEA) region, with catalytic converters the prime target. In the last 18 months, thefts of catalytic converters have been reported to the TAPA EMEA Intelligence System (TIS) in France, Germany, and the United Kingdom as well as in South Africa. While most crime reports stating this product type do not share financial loss data, these are known to be significant, high value incidents.

Yet, as with so many other types of cargo crime, the number of recorded thefts is believed to represent only a small minority of the total number of incidents taking place.

Spoofing is often used to trick victims into revealing sensitive data or to carry out ransom negotiations while concealing the identity of the attacker. Criminal networks may even offer spoofing services to other criminals.

In cargo transportation, criminals commonly employ GPS spoofing to manipulate the displayed location on a driver's device, leading them off their intended route and making them vulnerable to attack.



- **Theft from Moving Vehicles (internal and external)**

It was ten years ago when Europol warned about a new phenomenon where criminals use a 'Trojan horse' method to gain access to delivery lorries by concealing themselves in large wooden boxes. The boxes marked as 'Fragile' are picked up by parcel delivery services. Once the box is inside a lorry, route to its final destination, the criminals escape from the box to steal valuable items also inside the lorry, such as jewellery, phones, or electronics. Accomplices following from a distance then simulate an accident to stop the vehicle, enabling those hidden inside to escape via holes cut out of the vehicle roof.

Cargo thefts involving simulated accidents are quite common and thefts from moving trucks have also been reported on a regular basis. However, the Trojan horse modus operandi outlined above was at that time a new phenomenon.

Another interesting modus operandi is the one which criminals follow the moving truck at the same speed. They position themselves in the truck's blind spot, typically at the rear, where the truck driver cannot see them in the mirrors. They then climb onto the trailer, cut the seals on the lorry's load, and board the vehicle to carry out the theft. Accomplices follow at a fixed very small distance behind the attacked truck to receive the goods stolen. At the end of the attack, the onboard attackers return to the home-vehicle and slow down to get away from the truck.

### How to respond to a Deception Threat?

#### DOs




- If you are suspicious about the legitimacy of police or other authorities that stop you, within your route:
  - Call the police to confirm the legitimacy of the stop and inform them about your concerns.
  - Always inform your dispatching/monitoring centre about a sign from authorities on the road that ask you to stop your vehicle.
  - Request that the authorities accompany you to the nearest police station for necessary checks while keeping your dispatching/monitoring centre informed.
- Install a high security lock to avoid cargo compartment door opening while driving.
- Install sensors to inform you when the rear doors are open when underway.

#### DON'Ts

- **DO NOT** blindly trust individuals claiming to be police or other authorities without verifying their credentials or identification.
- **DO NOT** deviate from your planned route or change delivery locations, without confirming with your dispatching / monitoring centre.
- **DO NOT** hesitate to report any suspicious incidents or concerns to the police, your dispatching / monitoring centre, and relevant authorities.

## How to report a Deception Threat?


If you are stopped by police or other authorities for any checks, contact immediately your dispatching or monitoring centre and provide information about:

-  Your location.
-  Type of authorities (if possible).
-  Any vehicle license plate or other characteristics of the authorities.

## Hijacking

### What is Hijacking Threat?

Hijacking is to steal (cargo) from a truck or other vehicle after forcing it to stop, i.e. to hijack a load of tobacco. It also means to rob a vehicle after forcing it to stop, often instead of violence. Hijacking incidents pose a significant risk to drivers, with the potential for serious injury or even fatality.



**TAPA** EMEA<sup>®</sup>  
Transported Asset Protection Association

Thorsten Neumann highlighted three extreme contributors to the data presented for the first three-quarters of the year. These included €300 million of losses recorded in just two crimes; one involving the hijacking of miscellaneous goods in Belgium, and the other a case of fraud detected within a metal supply chain by a global organisation based in Germany.

### How to prevent Hijacking Threat?

- **Be aware during the driving time**  
As in the definition, in hijacking situations the truck needs to stop for the criminals to take control of it, therefore the most important way to avoid hijacking situations is not to stop when these situations are obvious and imminent. For instance, if individuals who do not appear to be legitimate authorities ask you to stop on the road, it is important to exercise caution and prioritize your safety. Even individuals posing as fake police officers or other authorities can pose a risk.
- **Recognition of Emerging Threats**  
It is crucial to be vigilant and prepared to handle hostile situations. Usually, hijackers either follow you before they try to take control of the vehicle or drive in front of you at a constant speed to monitor your driving behaviour.

## How to respond to Hijacking Threat?








### DOs

- Keep all doors and windows locked while driving.
- Stay alert and be aware of your surroundings. Pay attention to any suspicious or unusual activities, vehicles, or individuals.
- Try to create distance between your vehicle and the suspicious vehicle, so in case they stop you are able to make a manoeuvre and drive away.
- Maintain regular contact with your dispatching/monitoring centre or other designated contacts and share with them updates on your location and any deviations from the planned route.

### DON'Ts

- **DO NOT** allow any person to ride in your cabin.
- **DO NOT** stop and get out of the vehicle unless you have confirmed the validity of authorities that asked you to do so.
- **DO NOT** resist or confront the hijackers.
- **DO NOT** make sudden or suspicious movements.
- **DO NOT** provide unnecessary information to the hijackers.

## How to report Hijacking Threat?

-  After a hijacking incident, it is crucial to report the incident to the police and your dispatching/ monitoring centre as soon as it is safe to do so. Provide them with all relevant details to aid in the investigation:
-  Time/date/location of the incident and your current location (if different from the incident's location).
-  Any injury or need for emergency health support.
-  Name of driver/license plates of truck/trailer.
-  Number of criminals involved.
-  Type of authorities (if possible).
-  Any vehicle license plate or other characteristics of the authorities.

# Illegal Immigrants Entry

## What is Illegal Immigrants Entry Threat?

Illegal immigrant entry threat refers to the issue of unauthorized individuals attempting to enter countries by hiding in road freight vehicles. While illegal migration occurs globally across various transportation modes, the European migrant crisis has particularly impacted land transportation, specifically road and rail freight transport.

Criminal networks involved in migrant smuggling pose a significant threat, with some networks solely focused on facilitating illegal border crossings through road freight vehicles. This poses numerous challenges and risks for road freight transportation companies. Some of the consequences include property and cargo damage, physical and psychological violence against drivers, and other related issues. Furthermore, in cases where the cargo is pharma or food products, any intrusion of illegal immigrants into the cargo compartment or partial opening of packages are considered as contamination of it, and the cargo is rejected from delivery.

Currently, the debates over the problems caused by illegal immigrants to European road freight transport companies are not widely addressed.

### Case example

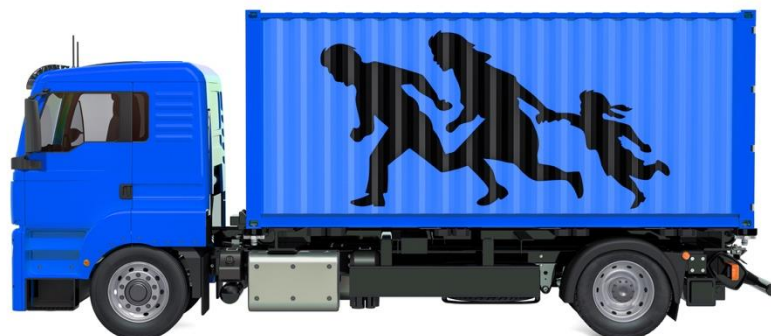
#### CRIMINAL NETWORK CHARGING UP TO EUR 20 000 PER MIGRANT

A criminal network facilitates the entry and secondary movements of irregular migrants in the EU. Migrants pay enormous sums to the smugglers to enter the EU clandestinely and move on to further destinations within its borders. The entire journey from the country of origin to the EU costs between EUR 15 000 and 20 000. The criminals advertise their illicit activities on various social media platforms to lure migrants, also by posting videos of successful transports. Migrants are moved along two main routes, either from Croatia via Slovenia to Italy, or from Serbia via Hungary to Austria.<sup>25</sup>

## How to prevent Illegal Immigrants Entry Threat?

Vehicles' checks before and after every stop

It is common for illegal immigrants to attempt to enter a vehicle when it is stopped or parked. To prevent this, it is highly recommended to perform vehicle checks before and after each stop. This practice involves walking around the vehicle and ensuring that there are no signs of attempted entry in the cargo compartment, verifying the integrity of seals, and confirming that all doors, locks, and closures are properly closed and secured.



## How to respond to Illegal Immigrants Entry Threat?

### DOs

- Be present when your truck is loaded.
- Seals and locks/padlocks are locked/fixed properly immediately after loading.
- When taking over the responsibility for the vehicle, you should ensure that the vehicle does not contain unauthorized persons.
- Check your vehicle and trailer for any irregularities prior to continuing your journey. Seals, locks, doors and canvas are in good condition and have not been tampered with.
- Always check perimetrically your vehicle after a short or long break to confirm there are no signs of intrusion and the seals and the locks are intact.
- Check any external storage compartments, axles, toolboxes, wind deflectors and the vehicle underside.

### DON'Ts

- **DO NOT** use unclassified parking locations for short and long breaks in areas where the risk of illegal immigrants entering your vehicle is high.
- **DO NOT** plan a break / overnight stay in remote areas (e.g. industrial zones, lay-bys).
- **DO NOT** make unnecessary stops while driving, especially if there are no scheduled stops or emergencies.
- **DO NOT** stop immediately if other persons signal you to do so (e.g. for a „problem“ with your vehicle).
- **DO NOT** open the trailer/vehicle.
- **DO NOT** approach the stowaways, keep distance.
- **DO NOT** touch the cargo / trailer, as there is a risk of contamination.

## How to report Illegal Immigrants Entry Threat?

If you witness or suspect an illegal immigrant entry threat, immediately contact the local law enforcement agency or emergency services in your area.

- 📍 Provide them with all relevant details,
  - the location
  - the number of individuals involved
  - any identifying information about the individuals involved
- 👤 Inform your dispatching/monitoring centre, or the appropriate personnel within your company about the illegal immigrant entry threat.
- 📋 Follow your company procedures.

## Last-mile Vehicles Crime

### What is Last-mile Vehicles Crime Threat?

Last-mile vehicles crime threat refers to criminal activities that target vehicles typically used for last-mile delivery in urban areas. These vehicles, such as minivans or smaller boxed trucks, often make multiple stops to deliver or pick up small parcels. Last-mile vehicles are particularly vulnerable to these types of crimes due to the frequent stops and the valuable contents they carry.

### How to prevent Last-mile Vehicles Crime Threat?

- Fit-for-purpose security systems on vehicles (auto-lock, RFID bands, etc.)  
There are a lot of fit-for-purpose security systems to prevent this kind of incidents, but the most important measure is to always lock all the doors of the vehicles and arm the security systems installed (intrusion vehicle alarm, immobilizer, etc.).

There are some very advanced security systems in place lately (for example RFID straps on the driver's wrist that automatically lock the doors of the vehicle and arm all security systems when the driver moves away at a certain distance from the vehicle (i.e. 3-5 m). These straps also unlock the vehicle's locks when the driver reaches a specific distance from it.

## How to respond to Last-mile Vehicles Crime Threat?

### DOs

- Always lock your vehicle and activate all security systems when you stop to make a delivery.
- Be vigilant and be aware of your surroundings.
- Identify suspicious behaviour or individuals and report any unusual incidents to your monitoring / dispatching centre.
- Carry a remote to activate the siren of the vehicle alarm system in case you see from a distance that someone either has entered your vehicle or tries to get in it.





### DON'Ts

- **DO NOT** park far away from the delivery point and have to walk a long distance with the parcels in hands to reach the delivery point
- **DO NOT** overload yourself with parcels when exiting your vehicle for delivery, so your hands are busy, and you try to close the vehicle's doors with your leg.
- **DO NOT** leave your keys in the ignition or unattended inside the vehicle, even for a short period.
- **DO NOT** leave any valuable items, including personal belongings or high-value parcels, visible from outside the vehicle.
- **DO NOT** share specific delivery information, such as the exact contents, addresses, or delivery schedules, with individuals who are not authorized or involved in the delivery process.

## How to report Last-mile Vehicles Crime Threat?

Reporting a last-mile vehicles crime threat / incident is crucial for addressing the situation and ensuring the safety of yourself, your vehicle, and the parcels being delivered.

Here is how you can report such incidents:

-  Immediately notify the local law enforcement agency or emergency services in your area.
-  Provide them with all relevant details, including the location, description of the incident, and any identifying information about the individuals involved.
-  Report the last-mile vehicles crime threat to your dispatching/monitoring centre or the appropriate personnel within your company.
-  Try to preserve any evidence related to the incident, such as photographs, videos, or any physical evidence that may be useful for the investigation



## Cybercrime and Information Security Leak

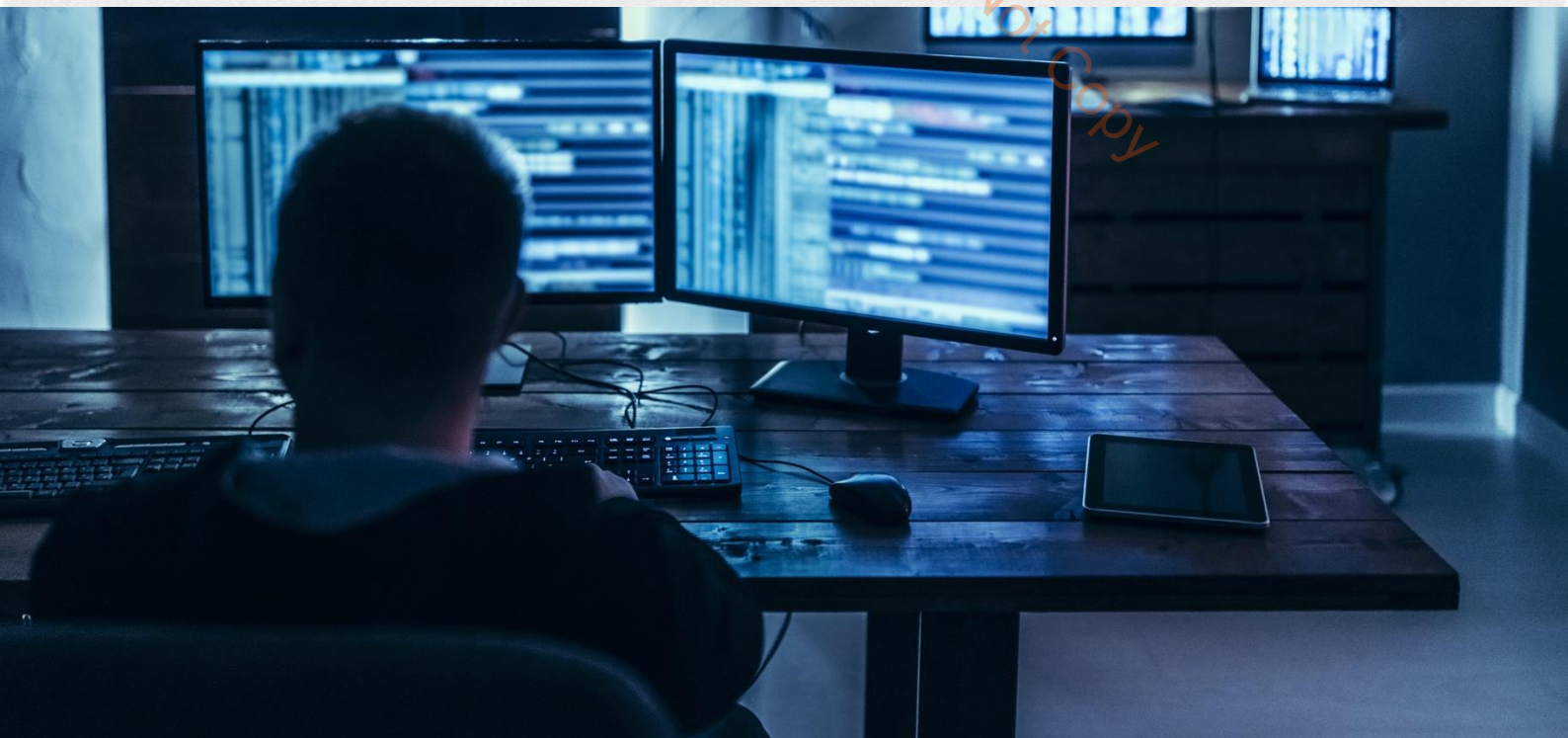
### **What is Cybercrime and Information Security Leak Threat?**

In Supply Chain Security when we talk about Cybercrime, we mean either attack to information systems targeting the stealing of sensitive cargo information (i.e. route origin and destination, types, and values of cargo) or unintentional information leak by the Logistic Service Providers or the drivers. In this document we shall focus on unintentional leak of information from drivers via their social media accounts or email accounts.

### **How to prevent Cybercrime and Information Security Leak Threat?**

It requires strong defence measures, with the understanding that human oversight remains the weakest link. Criminals often exploit vulnerabilities through phishing emails, malicious document files, social engineering techniques, and unpatched software and hardware.

- Be vigilant for phishing attacks on phones and tablets  
You should always validate incoming emails, especially those that ask you to use a link to proceed further. This way, criminals can access information stored on your phone including route and cargo details.
- Protection of Shipping Info and Documents  
Criminals can effectively organize an attack by gaining access to shipping documents, which contain vital information. For instance, a CMR document includes details such as the cargo's origin, destination, type, quantity, driver's name, seal number, and more. If criminals target your cargo, having access to this information is enough for them to start organizing the attack.
- Need to know basis  
Shipping documents is not the only way for criminals to get access to above info. Many times, the uncontrolled distribution of this information (either verbally or in writing) among employees, especially those that should not know this information, is adequate for a properly trained people to extract this information and provide it to the criminals' groups.



## How to respond to Cybercrime and Information Security Leak Threat?

If you suspect information leak either from computer systems or from uncontrolled documentation, you need to report this to your dispatching centre and ask them for instructions on how to mitigate its consequences.

## How to respond to Cybercrime and Information Security Leak Threat?

### DOs



- Always check the sender details before you click on a link in a received email.
- Protect shipping documents while they are under your custody.
- Report any unusual behaviour of your mobile phone and ask your IT dept. to check it.
- Report any suspicious activities or incidents to your organization's IT department or security team.
- Use strong, unique passwords for all your accounts and mobile telephone access.

### DON'Ts

- **DO NOT** answer any incoming call from unknown (usually from overseas) numbers.
- **DO NOT** share any information about your routes, including cargo type, estimated value, origin, destination, and break stops, with individuals who do not require this information.
- **DO NOT** publish job-related information and pictures in social media.
- **DO NOT** leave your devices unattended or unlocked, especially in public places.

## How to report Cybercrime and Information Security Leak Threat?

If you suspect you have fallen a victim of cyber-crime related to your transport route or you recognized a leak of details of your itinerary, report it immediately to your dispatcher/supervisor. In your report, include below details:

-  How you identified the leak or suspected cybercrime.
-  What specific information was leaked or compromised.

# Dispatching or Monitoring & Response Centres Functionalities and Support to Drivers

---

Monitoring & Response Centres play a crucial role in ensuring the safety and security of assets, such as trucks or trailers, during transportation. It is important to understand the distinction between tracking and monitoring:

- **Tracking:** Tracking refers to knowing the status or location of your truck and/or trailer. It provides real-time information on the vehicle's whereabouts, allowing for visibility and tracking its movements.
- **Monitoring:** Monitoring goes beyond tracking by comparing the actual status of your truck and/or trailer, such as its location, with the planned or expected status. It involves having a predefined plan or route and continuously comparing the actual data provided by the tracking system with the expected data.

It is important to note that monitoring can only occur when there is a predefined plan or route in place. Without proper planning, there is nothing to monitor. Therefore, monitoring centres rely on accurate planning and real-time tracking information to effectively monitor the progress and security of assets during transportation.

Please note that even in transports that there is no dedicated monitoring function to supervise the execution of the route, there is always a kind of supervision from the carrier's dispatchers towards the drivers and the cargo to ensure that there are no unexpected events during the transport. Therefore, always consider that there is someone at the home office or the monitoring centre that looks after your safety and cargo security.

The route is a combination of:

- a truck (with the trailer, if applicable),
- a driver,
- an origin,
- a destination,
- a time of departure,
- an estimated time of arrival, and
- Planned stops at pre-defined locations with associated time intervals for each stop in between.



There are several techniques / modes of monitoring:

- **Active Monitoring:** The monitoring station actively tracks and monitors the asset's location and progress throughout the entire duration of the route in real time.
- **Passive Monitoring:** The monitoring station checks and records the execution of the route once, or a few times during its duration.
- **Monitoring by exception:** The monitoring station receives alarms or notifications only when there are deviations from the planned route or schedule.
- **Monitoring per time-interval:** The monitoring station checks the execution of the route at regular time intervals, such as every 15, 30, or 60 minutes. It verifies whether the asset is following the planned route and adhering to the expected schedule within these predefined intervals.
- **Monitoring per route milestone:** The monitoring station checks every specific milestone (i.e arrival at a specific location to ensure that the route is being executed according to plan.

In principle the responsibility of a monitoring station is to:

- Receive,
- Verify, and
- Respond to an alarm event (any deviation from the planned route) within an agreed time interval.

Verification is typically conducted through phone communication between the monitoring station and the driver, using a specific key-word. The driver is required to include the key-word in their response to identify themselves and confirm their status. However, in high-risk routes, the driver may be instructed to exclude the key-word in the event of a real alarm, such as being under a hostage situation.

When the driver is able to communicate with the monitoring station, it is crucial for them to provide accurate information. This ensures that the operator at the monitoring station can fully understand the situation and initiate the appropriate response protocol.

In the case of a driver being under a hostage situation, predefined response protocols must be in place. These protocols consider that the driver may not be able to provide an accurate description of the situation due to the hostile circumstances. The monitoring station will initiate the necessary response actions based on the established protocols to ensure the safety and security of the driver and the cargo.

# European Emergency Contact Numbers

Country	Police	Emergency/Ambulance Services
Austria	133 or +43 59 133	112
Belgium	101	112
Bulgaria	112 or 166 or 02 98 28 363	112 or 160
Croatia	112 or 192	112 or 194
Cyprus	112 or 199	112 or 199
Czech Republic	112 or 158	112 or 155
Denmark	112 or 114	112
Estonia	112	112
Finland	112	112
France	17 or 112	15 or 112
Germany	110	112
Greece	100 or 112	166 or 112
Hungary	107 or 112	104 or 112
Ireland	112 or 999	112 or 999
Italy	112 or 113	112 or 118
Latvia	110 or 112	113 or 112
Lithuania	112	112
Luxembourg	113	112
Malta	112	112
Netherlands	112	112
Poland	112 or 997	112 or 999
Portugal	112	112
Romania	112	112
Spain	112 or 091 or 092	112 or 061
Slovakia	112	112 or 155
Slovenia	112 or 113	112
Sweden	112	112
Switzerland	117	144
UK	999	999 or 111



## Drivers' Valuable Rules

**You are transporting goods that might be targeted by organized or opportunistic criminals. To protect you and your freight follow the instructions below without any exceptions:**

1. Use the Expressway/Highways for long-distance journeys to major destinations. If possible, avoid the use of secondary roads and shortcuts.
2. Drivers and attendants should not relate, discuss and/or release any information regarding their consignment to any other party or persons whilst enroute to their destinations. Disclosure of job related information (routes, cargo, etc.) in personal social media accounts should also be avoided.
3. Never carry unauthorised passengers. Never pick up a hitchhiker.
4. Always keep your vehicle secure, even when driving.
5. Never leave the vehicle or shipment unattended at any time. Comfort breaks (such as meals and/or restroom breaks) shall not waiver this process – if two drivers are onboard, one of them must remain with the vehicle at all times. If the vehicle must stop for an extended period of time, check with dispatch or monitoring centre to ensure that you only park in approved secure locations, such as certified parking areas, toll plazas or at police stations in smaller towns or villages. Travel in convoys when possible.
6. If unavoidable to park outside a secure / protected area, take additional security measures like parking with the rear doors against another truck or walls.
7. If delivery cannot be accomplished, then advice must be sought from home-base or monitoring centre on what to do with the load.
8. Always insist on clear, precise POD signatures. Driver to check the ID of the person accepting the goods on behalf of the customer prior to handing over any packages. Challenge any last-minute changes.
9. Treat unsolicited offers of assistance from unknown person/s with caution.
10. Treat signals from other drivers that something is wrong with your vehicle with extreme caution.
11. Criminals sometimes pose as police officers or other government officials; therefore, additional attention should be paid when unexpectedly challenged by officials. Drivers should notify their dispatch or monitoring centre of their location prior to stopping their vehicle if safe to do so.
12. Keep in regular contact with dispatch/base. The driver should have multiple methodologies to contact dispatch/base (e.g. teletype, cellular phone, RF radio, etc.). Driver to carry mobile phone or other communication device at all times.
13. Watch your mirrors and take note of any vehicles that may be following your truck. Report any suspicious vehicles or incidents at the time.
14. Be in possession of a driver's security information card including all emergency contact numbers.
15. Be vigilant when accepting incoming calls or emails from unknown numbers / accounts.

**Do never break the rules. These rules are the basis for taking over the freight and doing the transport!**

# References

1. European Parliament study on Organized Theft of Commercial Vehicles and their Loads in the European Union
2. International Journal of Retail & Distribution Management Vol. 43 No. 3, 2015 pp. 204-220, Cargo Theft at non-secure parking locations, ©Emerald Group Publishing Limited, 0959-0552, DOI 10.1108/IJRDM-06-2013-0131
3. TAPA EMEA, 18 MONTHS OF CARGO CRIME EUROPE, MIDDLE EAST & AFRICA REGION, REPORTING PERIOD TO 30 JUNE 2022
4. The International Journal ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES ISSN 2345-0282, 2018 Volume 5 Number 3 (March) PECULIARITIES OF ILLEGAL IMMIGRANT'S INTRUSIONS INTO ROAD FREIGHT TRANSPORT UNITS IN THE FRANCE - UK CORRIDOR
5. Europol DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS, PDF | ISBN 978-92-95236-25-7 | DOI: 10.2813/811566 | QL-05-24-250-EN-N
6. Cyber-Security and Information Warfare, Copyright © 2019 by Nova Science Publishers, Inc. pp. 201, A Case Study Analysis of Attacks and Losses in the Supply Chain with the Use of GPS or GSM Jammers by the Attackers Panayiotis Laimos, Michalis Chronopoulos, Chrysanthi Laimou and Nikoleta Atanasova, ISBN: 978-1-53614-386-7
7. <https://www.fleeteurope.com/en/technology-and-innovation/global/features/ransomware-rise-again-causing-shattering-damages-fleets?t%5B0%5D=Fleet%20Management&curl=1>
8. Europol Internet Organised Crime Threat Assessment (IOCTA) 2023, Luxembourg: Publications Office of the European Union, 2023, PDF ISBN: 978-92-95220-83-6 ISSN: 2363-1627 doi:10.2813/587536 QL-AL-23-001-EN-N, © European Union Agency for Law Enforcement Cooperation, 2023
9. <https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/> Ransomware attacks on the transportation industry, 2021
10. <https://www.telegraph.co.uk/news/uknews/immigration/11694134/Calais-crisis-Illegal-immigrants-shut-down-all-Channel-traffic.html>
11. BSI and TT Club 2023 Cargo Theft Report, April 2024

## Disclaimer for the Driver Security Guide

This Driver Security Guidance Document provides helpful tips and information compiled to the best of our knowledge and belief, based on experience and background information. Topics have been selected according to current trends and necessities in 2024, elucidated, and published by TAPA EMEA. The association acts as a supporter of the industry and the connected supply chain in this context, aiming to minimize the possibility of losses from the risks mentioned herein.

Please note that the number and listing of the points mentioned may not be exhaustive, and not all potential dangers or further hazardous risks are listed here.

The recommendations regarding actions to avoid or proper behaviours mentioned in the document also reflect the expertise of TAPA EMEA experts involved in creating the present Driver Security Guide Document.

This document serves solely as support and a sensitization measure for General Cargo & HVC drivers. The responsibility for implementation, proper use, and correct application remains with the reader, user, or industry, including the logistic service providers.

The user/reader of the document/policy is aware of the associated actions. Neither TAPA EMEA nor the contributing experts incur any obligation, liability, or responsibility in tort relating to the topics mentioned herein, their handling, or the data provided, which is based on trust in references mentioned and provided by third parties.

### **Publishing and copyright information**

The TAPA EMEA copyright notice displayed in this document indicates when the document was last issued.

@ TAPA EMEA 2024

No copyright without TAPA EMEA permission except as permitted by copyright law.

### **Publication history**

First published in June 2024.

The (present) edition was published in June 2024.

