OVERHAUL

A Strategic Solution to Strategic Theft

Overhaul's guide to identifying & preventing theft by fraud

Introduction

Whether you call it strategic theft, theft by deception, or something else entirely, theft by fraud is a growing problem that entails unique issues not traditionally seen in straight cargo thefts. Whereas straight theft requires the physical presence of bad actors in order to commit theft - such as by tracking the shipment and waiting for an opportunity to steal it - theft by fraud involves manipulating shipment activity from a distance, nowhere near the actual goods, by using deception and trickery. Those who utilize such a method of theft have been identified as being highly skilled and generally more savvy regarding legitimate logistics and transportation methodologies than straight theft perpetrators.

Combatting theft by fraud requires a united effort because these new tactics are not as familiar to shippers, which makes it more difficult for them to determine the best defensive strategies. For that reason, Overhaul has put together this white paper on how to best identify and stop strategic theft in its tracks.

We begin by outlining common signs and examples of this type of theft before exploring both how and why it's on the rise. We then break down the various methodologies and show how a shipper can prevent fraudulent activity by asking the right questions, adhering to strict protocols, and enlisting the aid of an in-transit risk management partner. Finally, we explain how Overhaul is uniquely positioned to assist in that effort.

The ultimate desire is that this white paper helps shippers better understand the unique nuances of theft by fraud, why it's a growing problem, and how to take steps to avoid it. With this information, shippers can feel confident that they are playing a bigger role in keeping their company and the greater industry informed, prepared, and protected.

History of Theft by Fraud

Theft by fraud is nothing new to the industry, but the extreme effect it's having is fairly recent. Alongside pilferage, it is the fastest growing modus operandi (MO) of cargo theft in the US. Per dollar value, it has the highest impact.

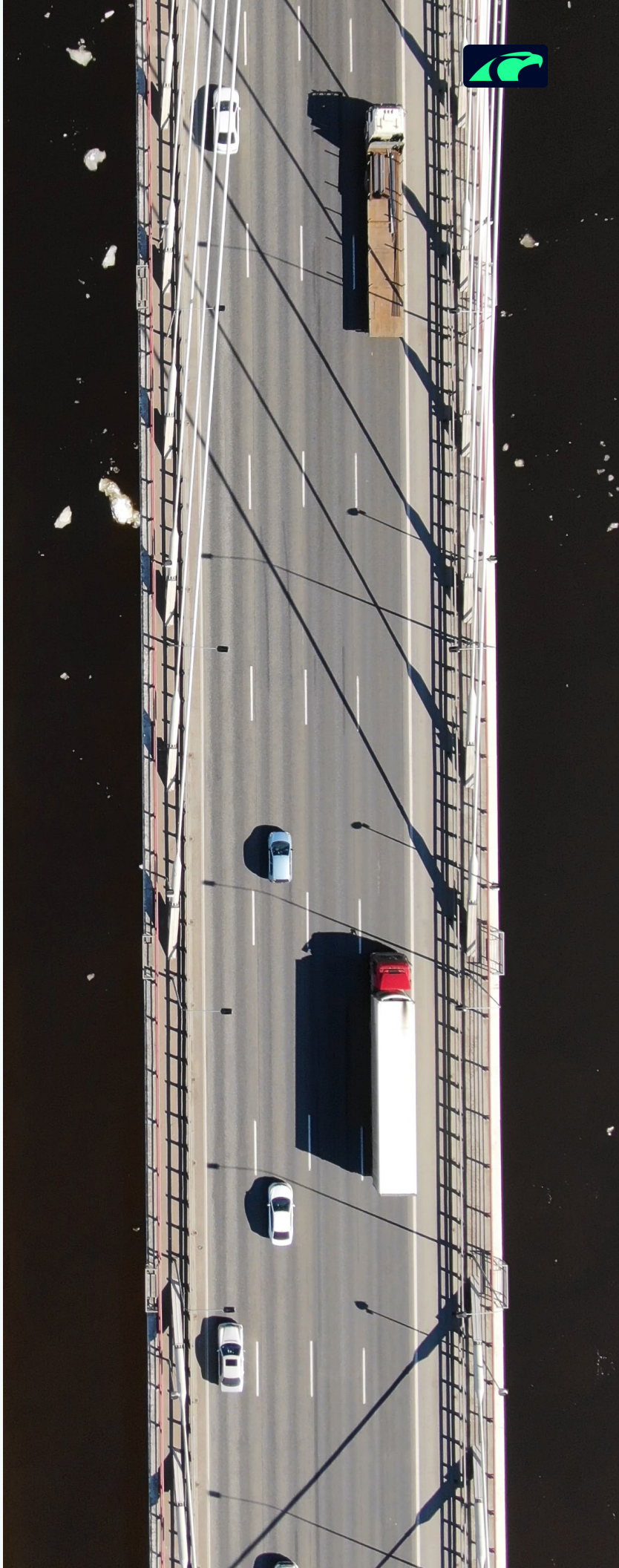
This theft used to be called fictitious pickup and would involve thieves using social engineering and inside information in order to steal cargo. Due to the lack of knowledge around these types of thefts, drivers who showed up claiming to be from the assigned carrier were not challenged.

While actual fictitious pickup is still an issue in some places, it has largely taken a backseat to other, more sophisticated thefts by deception. Some of these include buying inactive DOT/MC numbers and setting up fraudulent carriers or brokers. The most recent tactic has involved altering BOLs and delivering loads short.

In order to recognize and prevent theft by fraud, it's important to understand the following:

1. Structural Setup
2. Infiltration of Logistics Operations
3. Criminal Modus Operandi
4. How Stolen Freight is Turned into Dollars

There is an overlap between the four components outlined above. However, given the sophistication of criminal groups, these four aspects will provide clarity regarding why theft by deception is so complex and difficult to combat.



Structural Setup

Structural setup refers to the manner in which criminal groups organize themselves within the logistics industry and put themselves into a position to steal freight. This step can take on several forms and often involves insider knowledge and connections, as well as strategic planning.

1

Setting up Trucking/Brokerage Entities

Criminal groups are now establishing trucking/broker entities, specifically with the intent to steal cargo. These groups are well-versed in new entity setups, insurance, and all of the associated regulations. Setting up a new trucking entity under state and federal regulations can be done literally within a matter of days. Once established, the criminal groups will operate these entities legitimately as a profit-making operation, often overseeing several trucking/brokerage companies at the same time. The criminal groups will patiently build a relationship with logistics providers to create a legitimate operational history. Once they establish that history, the perpetrators will seek out high-value loads within a logistics company's network and execute thefts.

2

Buying Established DOT/MC Numbers

The US Department of Transportation (DOT) assigns MC or motor carrier numbers to all transportation firms that operate commercial vehicles. These numbers are the unique identifiers that help to track a company's compliance and safety. Criminals now attempt to purchase established DOT/MC numbers in order to establish themselves as a legitimate company with an existing operating history. Hence, a DOT/MC number with years of operating history is very valuable to a criminal attempting to establish a legitimate reputation.

3

Trucking Company Infiltration/Buying Off Drivers/Employees

A less common but well-documented tactic used by criminal groups is to recruit drivers with the intent of getting them hired into well-established trucking companies. In this scenario, it is often hard to determine whether more than one individual inside the trucking company is involved in criminal activity. Additional versions of this tactic involve paying for information from employees that allows criminal groups to execute thefts. This could include dispatchers, warehouse staff, or drivers. Once the criminal groups have an employee working within a trucking company or brokerage, there are several different tactics they can use to steal freight.

Infiltration of Logistics Operations

A key element of strategic theft operations involves the criminal actors' ability to infiltrate logistics operations. Like the other aspects of strategic theft, this is not a one-size-fits-all scenario.

A common tactic is for an illicit trucking company to create a business relationship with a logistics provider and begin hauling their freight. Often, logistics providers will use a carrier to haul low-value freight and then, after a certain number of successful deliveries, move them to higher-value/sensitive freight. Some logistics operations have as few as a five-load minimum prior to a carrier being permitted to move more high-value freight. Once established and approved for high-value freight, a criminal carrier can begin orchestrating thefts.

In some cases, the criminal carriers will obtain the rights to move several high-value loads on a given day or over a couple of days. Collectively, once they have all of those high-value loads in their possession, the perpetrators will disappear with the loads and shut down their company. Post-investigations often indicate the company ownership and legal structure were murky, at best.

Another tactic is to deceive logistics operations by email phishing and ultimately impersonating a legitimate trucking company to get loads assigned. This tactic often takes the form of creating an email address that is very similar to that of a legitimate trucking company. Once the logistics operator is successfully deceived and a load is assigned, there are typically very few additional checks performed to ensure that the driver/company picking up the cargo is legitimate.

Criminal groups have also been known to get some of their team members hired on as warehouse staff, often through temporary employment agencies. Once inside, these employees strive to learn internal processes, as well as gain access to information that can be used to orchestrate thefts. One common tactic is for an individual to obtain information about a load, after which the criminal group will show up at the pick-up location with all the correct information (based on what the insiders have been able to learn) and take it. This is usually only discovered when the legitimate driver shows up to pick up the load – and it is found to be missing.

Criminal Modus Operandi (MO)

As previously stated, Criminals employ various MOs and procedures to steal freight. Since these MOs are constantly evolving, it is somewhat difficult to cover them in their entirety. However, a few MOs are seen fairly frequently, and as such, we have covered them here in detail.

- **Traditional Fictitious Pickup**

  As previously mentioned, when fraudulent or deceptive thefts first became a problem in the supply chain, the predominant method of theft was identified as being Fictitious Pickup. Mistakenly, many in the industry still utilize this designation as the catchall term for all strategic thefts.

  In this MO, criminals employ social engineering, and in some cases specific shipment information, to pose as the driver and carrier that are scheduled to pick up the shipment. Typically, the actual carrier, whose identity is being used, is unaware of the scheme being carried out in their name and may actually arrive to pick up the load as scheduled, only to find that "another driver" has already obtained it. While this method is relatively low-tech and should be relatively easy to identify and avoid, it still impacts shippers today who are not aware of the method and the best practices to prevent it.

- **Double Broker Scams**

  By virtue of carrier identity theft, once a criminal has obtained the rights to a shipment (for example, in a load board transaction), they then turn around and pretend to be the broker they just obtained the shipment from or, in some cases, just another broker. The perpetrators then "re-broker" the shipment to a legitimate carrier they've targeted, saying something like, "We have you on our approved carrier list. Wondering if you have any capacity?" The legitimate carrier has no idea what is going on. They sincerely believe the shipment arrangement is perfectly normal/legal. Hence, this has none of the indicators traditionally seen with Fictitious Pickups - because there is no awareness of any criminal intent by the broker.

  There is also no suspicion at the pickup point, as the carrier that arrives is, in fact, a legitimate carrier and genuinely has nothing to hide. Criminal groups who are proficient in this type of scam can and do register multiple carrier and broker identities at a time, often sharing one of several phone numbers and addresses for the various entities they set up within their network.

- **Transloading/Shell Game**

  This method is often employed in concert with other MOs (most often double brokering scams) as an effective defense against investigation. Transloading describes the process of moving the freight into a different trailer or container (not just repowering with a new tractor) and possibly producing a new (fraudulent) Bill of Lading for the load. Such a new BOL could help disguise the contents (changing the freight characterization to something like "freight of all kinds" or FAK) while also indicating a different origin and destination and legitimizing the criminal actor as the designated carrier. This can actually happen several times before the perpetrators feel safe enough to completely take charge of the stolen shipment. Without granular supply chain visibility, this strategy effectively "launders" the stolen freight, making it unusually difficult for law enforcement officers to detect.

- **Repacking Scam**

  Likely a precursor to the BOL Altering method detailed below, this method involved the unloading of pallets and unpacking of cases to remove cargo. The cases would then be repalletized and rewrapped to match the original shipping condition. The load would be delivered to the destination fully or partially short - but with the proper pallet and case count to match the shipment's altered paperwork.

- **BOL Altering**

  One of the more recent methods to increase in popularity is what we are referring to as "BOL Altering." In this MO, the bad actors already have knowledge of shipment origins and destinations and are familiar with the shipping procedures. When a full load is uplifted from origin, the original BOL is scanned and altered to reflect a new piece count, weight, and seal. The new recordings are consistent with what has been left in the trailer after a portion of the shipment is stolen.

  When the altered paperwork is presented at delivery (often at large, very busy, regional distribution centers that have rigid receiving procedures), the shorted load is counted as complete. The actual shortage is not detected until accounting and inventory processes reconcile the difference typically weeks or even months later. The criminals in these cases often have an awareness of this reconciliation delay and will work diligently to obtain and short as many loads as possible within that timeframe.

How Stolen Freight is Turned into Dollars

Similar to their infiltration tactics and MOs, criminals will employ multiple strategies in order to turn stolen freight into money. The most well-known method is simply selling the goods outright, but even this strategy can take on several forms.

For example, a criminal might sell illegal products such as stolen drugs on the black market or dark web. They might also attempt to sell high-value goods, such as technology products, through legal channels by obscuring their stolen origins. This could mean using online stores where they can fake their identities or attempting to pass off products as legally obtained to unknowing distributors. In certain instances, they might even break down the product and scrap it for parts.

Some criminals will try to smuggle stolen products into other countries - where it's legally and physically more difficult to recover them.

In other cases, a criminal might hold your shipment for ransom, in the hopes that you'll pay to get the freight back rather than risk losing it entirely. This tactic is especially effective when it comes to goods such as pharmaceuticals, where a company could be held liable for losing such a consumable product.

More concerning, criminals could use stolen goods to further their own nefarious schemes. For example, stolen weapons might be used by criminal gangs to commit more violent crimes. Or, the proceeds from stolen goods could be used in the furtherance of terrorist activity.

Why are these Thefts Increasing?

The global increase in theft by deception has long been in the making. No one issue is responsible; rather, it is the culmination of several factors that has led us to this precarious state. One especially prominent factor behind the increase in disruption is society's growing reliance on technology, which has led to spikes in cybercrime.

As the world has become increasingly more technological, it has also become increasingly open to vulnerabilities. Cyber intrusions, through such techniques as "social engineering" or "phishing," allow criminals to infiltrate a company in order to better understand its makeup and more readily access sensitive information. Perpetrators can then use the information gleaned to assume a company's identity, forge documents, or conduct other illegal activities.

In the last decade, commercial truck drivers have had those technological advances virtually thrust upon them. Many independent owner-operators are not well versed in cybersecurity best practices or red flags indicating phishing and/or social engineering attempts. This makes it even easier for these vulnerable carriers to have their identity compromised.

Another factor that has encouraged this increase in theft by fraud is the current fast-paced business climate, which worsened during the pandemic. While the increase in a business's cadence of marketing its products can be very profitable, it can also lead to taking shortcuts, becoming complacent, or being lackluster in reasonable compliance with good supply chain security practices. In other words, even if goods need to be moved more quickly, it shouldn't be at the expense of safety and security.

Other Reasons Criminals are Drawn to these Thefts

The aforementioned factors are by no means the only reasons why these crimes have spiked. The truth is, theft by fraud is an especially attractive crime for thieves because, again, it is conducted "at a distance" where the risks of exposure are far less than having to be present to take control of a shipment.

Lower risk

The nature of theft by fraud means that it can also be performed in a non-violent manner. Other freight crimes, such as hijacking, can involve everything from threats to physical harm. Conversely, with strategic theft, a criminal can conduct their affairs via electronic communications, which allows them to do much of their nefarious activity over the phone or online.

Hard to detect/prosecute

Theft by fraud can also be difficult to trace since it rarely involves "hands-on" activity, rather relying simply on manipulating business processes. In that way the actual detection of the crime takes time – more time than that involved in detecting a "straight" theft. Add to that, once the crime is detected a question almost always arises as to law enforcement jurisdiction – as to just when, as well as just where, did the fraud lead to the freight crime.

Harder to recover

Because this type of theft is hard to trace, it can make it difficult to recover stolen goods. Often in the commission of these types of fraud, new shipment paperwork has been generated, essentially "laundering" the cargo by providing new provenance. Worse, since theft by fraud can be conducted by anyone, anywhere in the world, recovery efforts can face both legal and jurisdictional hurdles. Although this new international wrinkle may seem to some as being rare, it is steadily becoming more commonplace and coordinated. Current intelligence has shown multiple criminal groups establishing fraudulent carrier identities from outside of the United States.

Scalable

A small group of people can take an entire day to commit straight theft, and in the end, they'll have stolen a single load. Conversely, one person with even average computer skills, having created a network of fraudulent carriers, can steal a dozen loads a day without ever actually touching the freight. No industry, region, or size load is immune to this type of activity. The more successful perpetrators become with this technique, the more scalable the methodology becomes.

Best Practices for Staying Safe

In order to keep your company protected, staying informed is essential. Taking the contents of this white paper to heart is a good start, but it's also important to continue to research and learn as much about the current evolving tactics as you can. You also need to share what you've learned with your employees and supporting vendors, as "they can't defend against what they don't know."

Regular training can help your employees identify and avoid theft by deception. Such training should cover everything from cybersecurity best practices to social engineering and phishing red flags. Testing your employees, with such things as fake phishing emails, is one way to see if you are getting through.

It's also important that you thoroughly evaluate all of the companies you work with, as well as inquire about how they assess their own partner companies. A business is only as strong as the weakest link, when it comes to supply chain activity. As an example, it's not enough for you to just assess your freight broker, but also to ensure that your broker is also vetting its selected carriers.

On a final note, criminals have been known to crave as much insider knowledge as they can obtain. Always be suspicious of: interest in your company from sources you are unfamiliar with, questions being asked of your employees as to how you do business, new employees that you are looking to hire, odd communications coming from generic sources, and business deals which seem to be moving faster than by traditional methods.

Theft by deception does typically present a number of "red flags." The more you and your company learn about them, the easier they are to spot. Know too that even the best procedures can have weak points and blind spots that prevent one from seeing the full risk landscape. This is why it's also critically important to work with an in-transit risk management partner.

Why Work with an In-Transit Risk Management Partner?

An in-transit risk management partner can help your company maintain visibility into its cargo and shipments, as well as share the latest risk-based intelligence. Through visibility, you'll be able to track your cargo and quickly identify any unauthorized access or tampering. These partners can also take advantage of other forms of the latest technology to help spot threats and risk in advance.

Of course, not all partnerships are created equal, and it's important to vet a provider before bringing them on board. To help you do so, here are some questions to consider:

1

What Features does the Provider Offer?

Certain companies require more visibility features than others. For instance, an LSP will want visibility into both its cargo and its assets. Additionally, companies who oversee global shipments will require providers that can monitor different modes of transportation and provide insight into theft patterns in all parts of the world. Perhaps most importantly, a good in-transit risk management partner should be able to not only identify strategic theft risks, but also help you respond to them. For these reasons, before choosing a partner, make sure your needs align with their offerings.

2

Is the Provider a Reliable Partner?

Your chosen risk management partner should offer the best customer experience possible. First and foremost, this means it must be reliable. In the world of supply chain security, trust can be a scarce resource. An in-transit risk management partner isn't worth much if you can't trust them to help keep your products protected. Reasonably, this also means listening to their advice and using their available tools as intended. Thus, before selecting a provider, it's important to talk to the people working there, request/read reviews, and more generally gain as full an understanding of what your working relationship would look like as possible.

3

Is the Provider Future-Focused?

As theft by deception continues to evolve, you and your chosen in-transit risk management partner must keep an eye on the future. This means not only being able to respond to current risks but also being aware of, as well as adaptable to, new and emerging threat patterns.

Every company is unique. Risks are never static. As your company grows your risk profile will, reasonably, grow as well. A good risk management partner should be adaptable to that growing risk, future-focused, and committed to helping you avoid threats and supply chain disruptions while still achieving your business goals.

How Overhaul Helps Companies Combat Theft by Fraud

Overhaul is a leading in-transit risk management partner that takes a different approach to supply chain safety/security. Alongside visibility, we also provide risk monitoring and compliance support. Together, these capabilities enable companies to not only identify risks but also take action against them in real time.

Bad Actor Alerts

Overhaul maintains and monitors our own first party list of bad actors. Through our Threat Intelligence Program - a tiered offering within our "Intelligence as a Service" platform - we have the capability to notify you immediately if one of our blacklisted carriers is looking at, or may be in a position to be tendered one of your shipments. This way, you can proactively prevent them from obtaining the rights to your shipment.

Intelligent Door Seal Solution

Overhaul's Intelligent Door Seal Solution integrates a smart door seal, incorporating Bluetooth and GPS, into the Overhaul platform. This solution notifies users when a trailer door is opened. More accurate than a light alert, the Intelligent Door Seal Solution can be a final line of defense against thieves in their attempt to access stolen cargo.

Shipment Manager

Overhaul's Shipment Manager provides comprehensive shipment visibility, which makes it easy to locate shipments, quickly determine their expected arrival times, and track their progress in accordance with set plans. These insights can help you quickly identify route or compliance deviations and take action to prevent a stolen load.

RiskGPT

The AI-backed RiskGPT significantly reduces cargo theft risks by improving incident response time and accuracy. It also provides for real-time responses. By relying on Overhaul's proprietary intelligence, RiskGPT is able to quickly provide support to customers experiencing unique events, such as those involving theft by deception.

LE Connect Program

The goal is always to prevent crime, but should a strategic theft actually occur, Overhaul's LE Connect technology connects cargo theft victims with responding law enforcement officers. Together, they work with Overhaul's global security operations center (GSOC) and Intelligence and Response teams to recover stolen cargo.

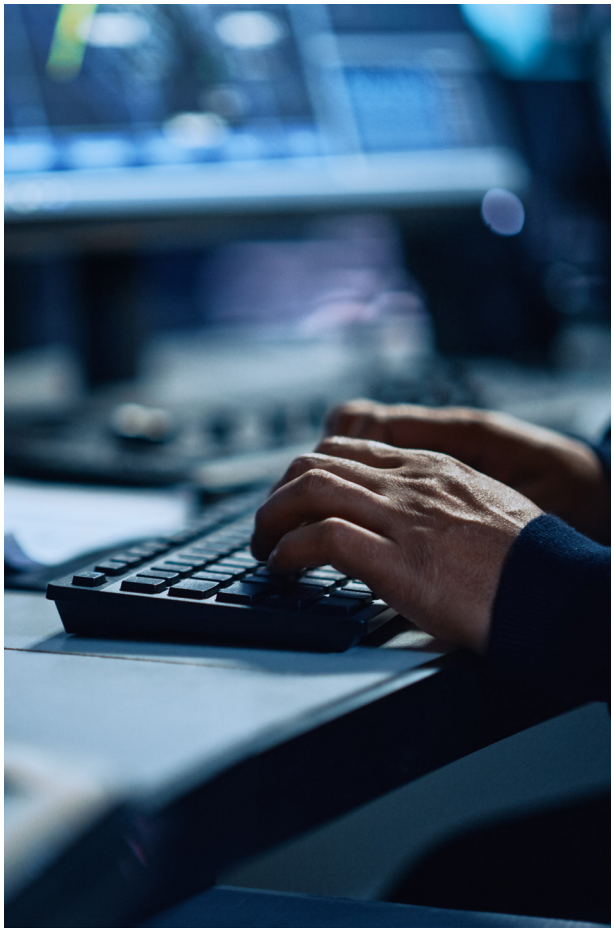
Cargo Insurance

Along with having a good recovery plan, having a good insurance plan can make all the difference in the event a theft/disruption does occur. Overhaul works with insurance providers to keep premiums down and streamline claims procedures. When our full solutions are engaged, this can lead to a reduction in loss rates up to 80%.

Everyone stands to lose when a strategic theft is pulled off successfully. The shipper loses their cargo, which can mean lost revenue and brand reputation. Innocent drivers might not be paid and could be marked by thieves as easy future targets. And consumers who wanted the products will have to wait for a new shipment, or else find a different provider. Worse yet, the successful criminals will feel empowered to continue their illicit behavior, which could mean further harm across the industry.

These crimes are continuously evolving. Thieves now use the internet, faxes, and phone calls to commit their schemes. They can also strike from anywhere in the world without having to expose themselves, which wasn't the case with previous theft methods. And because these criminals stand to gain so much, there is little reason to suspect that their thefts will decrease anytime soon.

Don't let theft by fraud fool you. With the right strategies and tools in play, you can greatly mitigate the risks of theft by deception and help keep your business and the greater industry protected. By working with Overhaul, you'll gain access to enhanced visibility, risk monitoring, and compliance support. Together, we can strategize against strategic theft and make a difference in the supply chain.



Reach out to our Sales Team at sales@over-haul.com to learn more about how we can help prevent theft by fraud.