Statement of

Adam Blanchard
Principal and CEO
Tanager Logistics and Double Diamond Transport

on behalf of

The American Trucking Associations

Committee on Commerce, Science, and Transportation
Subcommittee on Surface Transportation, Freight, Pipelines, and Safety
United States Senate

Hearing on

Grand Theft Cargo:
Examining a Costly Threat to Consumers and the U.S. Supply Chain

February 27, 2025

Introduction:

Chairman Young, Ranking Member Peters, and members of the subcommittee, I appreciate the opportunity to testify before you today on behalf of the American Trucking Associations (ATA).[1] My name is Adam Blanchard, and I am the Principal & CEO of both Tanager Logistics and Double Diamond Transport, headquartered in San Antonio, Texas. I am also a proud serving member of the Texas Trucking Association and am grateful for the opportunity to share with this subcommittee the challenges that I, my peers in Texas, and the trucking and supply chain logistics industry nationwide are experiencing with supply chain fraud and cargo theft.

ATA is a 90-year-old federation and the largest national trade organization representing the 8.5 million men and women working in the trucking industry. As a 50-state federation that encompasses 37,000 motor carriers and suppliers, ATA proudly represents every sector of the industry. From less-than-truckload to truckload carriers, from agriculture and livestock transporters to auto haulers and household goods movers, and from large fleets to mom-and-pop one-truck operators, ATA serves as the single unified voice of the trucking industry.

Since founding Double Diamond Transport and Tanager Logistics in San Antonio in 2014, we have been fortunate to grow the company to operate 90 trucks and employ over 20 freight brokers. As a full-service transportation provider, we offer reliable truckload transportation services using the latest technology and equipment to provide top-tier customer service. We are proud to have been recognized by Inc. Series 5000 as one of the fastest-growing private companies in San Antonio.

Our experience as both a trucking company and logistics provider has exposed us to the numerous ways in which bad actors are infiltrating our nation's domestic supply chains. We have seen how easy it is for criminals to create fraudulent trucking companies and brokerages and steal cargo from the stream of legitimate commerce with near impunity, all while undermining the integrity of the trucking industry. I have been a victim of freight fraud numerous times, and unfortunately there is virtually no recourse for me or my company. I look forward to sharing the challenges I experienced working with federal, state, and local law enforcement, as well as federal regulators, and discussing solutions to help our nation better combat supply chain fraud and theft.

Thank you for convening today's hearing to consider these critical issues. I, along with the ATA, look forward to working with you to share information and inform potential legislative solutions to promote the safe and efficient movement of our nation's goods.

What is Freight Fraud?:

Thieves, Organized Theft Groups (OTGs), and Transnational Criminal Organizations (TCOs) are currently infiltrating and exploiting the nation's transportation and distribution networks because these criminal schemes are considered low-risk and high-reward. In other words, there is significant money to be made and very little risk of criminal exposure. According to the National Insurance Crime Bureau (NICB), cargo theft in the United States is a $15 to $35 billion industry.[2] The fraud and cargo theft plaguing the trucking industry, and our nation's supply chains more broadly, materialize in many ways. There are two main categories of cargo theft: straight theft and strategic theft.

[1] The American Trucking Associations is the largest national trade association for the trucking industry. Through a federation of 50 affiliated state trucking associations and industry-related conferences and councils, ATA is the voice of the industry America depends on most to move our nation's freight.

[2] National Insurance Crime Bureau. On the Rise: Cargo Theft, a Billion Dollar Industry. https://www.nicb.org/news/blog/rise-cargo-theft-billion-dollar-industry.

Straight Theft

Straight theft is the most common form of theft and has been around for as long as trucks have been delivering freight. Straight theft refers to thieves physically stealing cargo from a shipment. Thieves typically target products that can be sold quickly on the market, and this type of theft can be very profitable. Examples include:

1. **Burglary**- Thieves steal goods directly from truck trailers, usually when truck drivers are stopped along their routes at truck stops, parking lots, roadside parking, terminals, drop lots, and other areas where cargo could be left unattended, especially in retail store parking lots or other empty parking lots on weekends.
2. **Pilferage**- Thieves only steal some of the freight off a single trailer. Criminals pilfer small amounts, often over long periods of time. By taking only small amounts of freight at a time, thieves are able to avoid detection for much longer and pocket hundreds or even thousands of dollars of merchandise without much effort or risk.
3. **Hijacking**- Thieves use force, deception, or intimidation to seize the truck and its contents. Thieves may trick drivers into pulling over by signaling that something may be wrong with the truck, which then allows them to steal the freight. OTGs may target entire trucks or containers by using violence or other tactics to overpower drivers and seize the cargo. This can be opportunistic, or a truck can be tracked from its departure point and robbed at its first stop.

Strategic Theft

Strategic theft involves the use of fraud and deception to trick shippers, brokers, and carriers into handing loads over to thieves instead of the legitimate carrier. Strategic theft often involves identity theft and advanced cyber tactics to manipulate data. Strategic cargo theft is extremely profitable and lower risk relative to straight theft because strategic theft can be accomplished remotely and does not require thieves to physically touch the cargo. Examples include:

1. **Fictitious Pickups** - Thieves impersonate legitimate drivers and carriers by using altered paperwork, fake uniforms, and vehicle logos to steal shipments. The legitimate driver will often arrive to find that the shipment has already been released.
2. **Fraudulent Bills of Lading** - Thieves use the forged identity of a legitimate carrier to pick up a shipment, steal a portion of the freight, and re-create the bill of lading to disguise the theft. In this process, the unit count, weight, and seal numbers are altered on the bill of lading before the shipments are delivered to the final destination, where the unknowing receivers sign off. This type of theft can go undetected for months.
3. **Double Brokering Fraud** - A double brokering scam can take various forms in the trucking and logistics industry. Sometimes, the criminals pose as either legitimate brokers or motor carriers (i.e. owning trucks, trailers, equipment, or drivers), or both, but they, of course, have no intention of moving the freight to the destination requested by the shipper. Instead, the criminals steal cargo by subcontracting the work to unwitting carriers who transport the freight to a different delivery point than the location specified by the shipper. The criminals do this by either convincing the legitimate carrier to deliver to a different destination or changing the bill of lading. Often, criminals engaged in double brokering fraud are not located in the U.S. and conduct their crimes through cyber means without ever physically touching the freight. It is also common for criminals to steal the identity of an existing broker or motor carrier by creating and using website domain names and business names that are very similar to the existing business information of real companies. For example, a real trucking company might use the website domain ABCMotorCarrier.com, and the criminal may create a fraudulent company with a

slightly different website domain such as ABCMotorCarrierLLC.com. There are multiple victims with double brokering scams: the owner of the double-brokered freight, the motor carrier that unknowingly delivered the freight for the criminal and won't receive payment for their service, and the legitimate broker whose operations and integrity are undermined by fraudulent actors.

4. **Hostage Freight** - Freight can be held hostage by a broker, carrier, or rogue driver. Hostage freight refers to scenarios where brokers, carriers, or rogue drivers refuse to complete a delivery until their demands are met. Drivers or service providers may hold loads hostage when they think they are not being paid fairly, or as a means to renegotiate the terms of the initial agreement. These situations can be complicated when associated with double brokering fraud. Hostage freight schemes are also fairly common in the moving and storage industry and occur when a moving entity holds a customer's belongings hostage by refusing to deliver them until the customer pays a significantly higher price than the original estimate. Thieves will use the customer's belongings as leverage to extort additional money. In many cases, the customer's goods are never returned even if the additional money is paid.[3]

USDOT & MC Number Fraud

The trucking industry and broader supply chain's growing experience with cargo theft is often tied to sophisticated fraud tactics undertaken by criminal organizations and lone bad actors. In many instances, these bad actors exploit vulnerabilities in the Federal Motor Carrier Safety Administration's (FMCSA) current carrier and broker registration system by stealing, falsifying, or creating counterfeit information to unlawfully acquire U.S. Department of Transportation (USDOT) numbers, Motor Carrier (MC) numbers, operating authority identifiers, and other critical data. USDOT requires the trucking industry to use these unique identifiers to ensure that only legitimate, authorized carriers operate on our roads.

Unfortunately, bad actors are increasingly targeting USDOT numbers, MC numbers, and other business identifiers to carry out their illicit schemes under the guise of legitimacy. Some common tactics include hacking into carrier databases, exploiting weak security practices, and phishing schemes. In some cases, these scammers create entirely fabricated carrier companies using stolen or purchased credentials. Fraudsters may register new companies using stolen information by extracting USDOT and MC numbers from publicly accessible databases or using phishing schemes to deceive companies into revealing sensitive information, including PINs and other personal details.

In other instances, they hijack existing carrier profiles by hacking FMCSA accounts via elaborate phishing schemes or online data mining. The fraudsters use the stolen credentials to establish a fake entity and alter legitimate company information in official records, like the MCS-150 form, to redirect communications to themselves. They then create websites and email addresses that closely resemble those of legitimate companies (i.e. spoofing), using fake phone numbers and emails to communicate with brokers and shippers and conduct what appears to be legitimate business.

Another common and concerning practice is the buying and selling of both stolen and legitimate business identifiers. It is relatively easy to find "black markets" online that feature USDOT and MC numbers in good standing. These markets often operate in plain sight on open Facebook forums and other public domains.[4] Importantly, the buying, selling, and transferring of MC numbers on its own is

[3] WTW. (2024, December 18). High-value shipments at risk: The growing threat of strategic cargo theft. https://www.wtwco.com/en-us/insights/2024/12/high-value-shipments-at-risk-the-growing-threat-of-strategic-cargo-theft.

[4] Examples of Facebook groups and domains where USDOT and MC numbers are exchanged: (1) "MC number buy/sell/assistance," https://www.facebook.com/groups/808090098179571; (2) "Operating Authority for sale (MC and

not illegal, so there are limited means to "police" this practice and stop bad actors from purchasing unique identifiers with malintent.[5] Additionally, trucking businesses are frequently purchased and consolidated, meaning the transfer of such credentials is inevitable and, in many cases, done for legal purposes. However, fraudsters often operate in a legal gray area by using legally obtained MC numbers to evade FMCSA's compliance guardrails and then conduct illegal operations.

Notably, fraudsters and cargo thieves specifically seek out the USDOT and MC numbers of companies that have strong safety records and established operational histories to both appear more credible and evade the scrutiny of law enforcement and regulatory bodies. By acquiring the business identifiers of companies with strong safety records, fraudsters can avoid certain compliance checks and bypass certain vetting processes that would otherwise expose them. Bad actors often offer registered carriers with excellent safety ratings tens of thousands of dollars to obtain their "valuable" MC numbers. They will pay even more to also obtain carriers' registration account credentials and other personal or business information to seamlessly infiltrate their established business networks.[6]

While domestic bad actors certainly play a role in targeting the vulnerabilities of FMCSA's current registration system, a significant amount of fraud originates internationally, particularly from TCOs and fraudsters operating in places like Eastern Europe, Central Asia, Southeast Asia, West Africa, and Latin America. These criminals often target U.S.-based registration systems to exploit the relatively easier access to legitimate identifiers like USDOT and MC numbers. Moreover, given how technology is embedded in nearly all aspects of the U.S. supply chain, it is relatively easy for bad actors in overseas locations to capitalize on technological vulnerabilities and perpetrate freight fraud.

My Experience With Identity Theft

Unfortunately, about a year ago, the business identity of my company, Tanager Logistics, was stolen by a bad actor. The identity thieves communicated directly with our business to tender a load on behalf of a trucking company and subsequently posed as Tanager Logistics to broker that load, as well as other loads, to motor carriers. While we still do not know today how exactly the fraudster obtained the sensitive business information that allowed them to impersonate our company, we believe they may have used publicly available information and setup packets to gain legitimacy. They brokered loads under our name, deceiving both shippers and carriers. This led to massive business disruptions, with angry trucking companies calling us and demanding payment for loads that the real Tanager Logistics did not broker or authorize. Worse, the fraudster used our identity to steal high-value freight, including truckloads of Red Bull, which were then diverted to suspicious warehouses in California and ostensibly shipped out of the country. Despite reaching out to our insurance provider, law enforcement, and even the Department of Homeland Security, we were met with indifference and red tape. The fraudulent actors used VPNs and domain spoofing techniques, making it nearly impossible for us to track them down on our own. This experience exposed a major flaw in the industry—there is virtually no recourse for businesses facing this kind of fraud. FMCSA and other regulatory bodies need stronger mechanisms to detect and respond to these scams in real-time. More importantly, federal agencies must prioritize cyber capabilities to track and shut down these criminals before they can continue defrauding legitimate businesses like mine.

USDOT)," https://www.facebook.com/groups/764465795015988; (3) "MC Number. Sale or buy," https://www.facebook.com/groups/742321597745830; (4) https://dotnumberstore.com/.

[5] Lockie, Alex. (2024, October 10). FMCSA guidance on buying and selling MC numbers. Overdrive. https://www.overdriveonline.com/regulations/article/15705499/fmcsa-guidance-on-buying-and-selling-mc-numbers.

[6] Lockie, Alex. (2024, September 30). How much is your MC worth? Maybe as much as $30,000. Overdrive. https://www.overdriveonline.com/channel-19/article/15704468/your-authority-might-be-worth-30000-to-freight-fraudsters.

To this day, FMCSA's SAFER website still features two companies under the name "Tanager Logistics LLC": my company—the real Tanager Logistics LLC[7]—and another fraudulent business[8] purporting to be my company. It is disappointing and aggravating that the federal agency responsible for improving the safety of the trucking industry routinely publicizes fraudsters on a system intended to share "company safety data to industry and the public over the internet."[9]

Industry & Broader Public Safety Impacts

USDOT and MC number fraud not only victimizes legitimate carriers, brokers, and shippers, it also poses significant risks to public safety. Illegitimate carriers often operate unsafe vehicles, hire unqualified and uncredentialed drivers, and avoid regulatory oversight altogether. In some instances, these bad actors also engage in fraudulent insurance practices, further compromising the safety and integrity of USDOT's registration system and industry norms. Criminals use stolen or unethically purchased numbers to facilitate illegal activities beyond cargo theft, including human trafficking and the transportation of illicit substances and goods. Thus, the impact of this fraud extends far beyond the trucking industry itself, threatening the U.S. marketplace, public safety, and national security.

Without the deterrence of reliable investigations and prosecutions, the trucking industry is constantly vulnerable to potential fraud, and legitimate carriers must expend significant human capital and financial resources to protect themselves. Unfortunately, many smaller carriers and brokers lack the means, staffing, and financial resources to make such robust investments needed to protect themselves and their customers' cargo. This Committee plays a key role in safeguarding our nation's transportation networks and supply chains. We urge you to consider how the prevalence of fraud and absence of any real deterrent undercuts the trucking industry's ability to enhance the safety and efficiency of our fleets to keep up with America's transportation and supply chain needs.

FMCSA's Actions to Combat Fraud

FMCSA established a dedicated fraud prevention team in June 2024 to identify and respond to suspected cases of motor carrier and broker fraud and assist registrants who have fallen victim to fraud.[10] While the team is still relatively new, FMCSA's goal is to play a role in actively mitigating the fraud that is occurring within the industry. The agency has also enhanced its practices and scrutiny around registration applications and documentation submitted via paper—a key source of many fraud incidents—and has begun transitioning towards more secure, encrypted online processes. Another short-term fix FMCSA has identified and undertaken is the suspension of online PIN requests to thwart fraudulent actors from using this tool to access the FMCSA registration system illegally. All PIN number requests are now completed by FMCSA mailing the information to a physical address on file.

FMCSA has also announced several planned upgrades to the registration system that build upon ongoing modernization efforts to further bolster security and deter bad actors. Importantly, FMCSA plans to eliminate MC and other operating authority numbers and instead require a single identifier (USDOT number followed by a suffix indicating operating authority type). While the move to consolidate these numbers into a single USDOT number is intended to simplify regulatory oversight and improve efficiency, it is also a key step in reducing fraud by centralizing carrier verification and compliance

[7] Tanager Logistics LLC. USDOT Number: 2543054
[8] Tanager Logistics LLC. USDOT Number: 4326934
[9] U.S. Department of Transportation. FMCSA. About SAFER. https://safer.fmcsa.dot.gov/about.aspx.
[10] Gallagher, John. (2024, April 24). FMCSA standing up registration fraud team. FreightWaves. https://www.freightwaves.com/news/fmcsa-standing-up-registration-fraud-team.

checks—moving away from siloed or one-off verification processes for multiple business identifiers. FMCSA believes a single-number system could help reduce vulnerabilities that allow bad actors to manipulate or steal MC numbers to deceive brokers and shippers. Other planned upgrades include the issuance of safety registrations that will be attached to the carrier's USDOT number, as well as more robust business verification processes and streamlined systems for identifying active and prohibited system users.

I, and ATA, strongly encourage the Committee to exercise robust oversight as these changes are put in place by the agency. While many of these updates will require formal rulemakings, the trucking industry welcomes changes to FMCSA's system that enhance security and deter fraud while maintaining user accessibility. In introducing these registration system enhancements, FMCSA must take caution to avoid creating undue administrative or regulatory burdens for carriers and brokers.

Organized Theft Groups and the Rise of Strategic Theft:

While cargo theft is not a new phenomenon, in recent years, it has evolved from a domestic enterprise into a sophisticated, international effort perpetrated by hostile entities. Organized criminal syndicates all over the globe have the means and wherewithal to create fraudulent trucking companies and brokerages and profit off vulnerabilities in U.S. supply chains, all without ever stepping foot on U.S. soil. These crime rings are predominately located in Eastern Europe, Africa, and South America. They continue to harm unsuspecting American companies, and ultimately consumers, because of the notable absence of any real deterrence (i.e. investigations, prosecutions, and justice).

The COVID-19 pandemic precipitated the meteoric rise in frequency and sophistication of cargo theft. CargoNet logged 1,106 reported incidents of theft in 2019 and 1,181 reported incidents in 2018.[11] During this time, the vast majority of reported thefts could be categorized as straight theft. These crimes were carried out by relatively unsophisticated thieves who would steal freight when the opportunity presented itself. These thieves would sell the stolen goods at a deep discount, usually pennies on the dollar, in the same area where the goods were stolen. The thieves would live off those proceeds until exhausting their resources, at which point they would strike again.

Beginning in 2021, however, the trucking industry saw a dramatic shift in the cargo theft landscape. Strategic theft has risen by over 1500% since the first quarter of 2021.[12] Unlike the thieves of the past who engaged predominantly in straight theft, those engaged in strategic theft utilize fraud and deception to maximize profit and maintain a safe, physical distance from the theft itself. These criminals are often members of OTGs that operate massive networks within and outside the United States. The shift from opportunistic thieves to large OTGs gave rise to more complex and convincing fraud operations. Less than a decade ago, when smaller and less sophisticated groups were apprehended by law enforcement, it would take around 6-7 months for them to restart theft operations. Nowadays, when law enforcement successfully disrupts a large criminal network, it takes 30 days or fewer for that group to resume their freight fraud operations because of the relative ease with which bad actors can reinvent operations online. The constant cycle of seemingly futile efforts to combat crime as criminals simply move their operations elsewhere resembles a game of "whack-a-mole."

[11] Wolf, C. D. (2021, June 10). Truck cargo thefts skyrocketed amid COVID-19. Transport Topics. https://www.ttnews.com/articles/truck-cargo-thefts-skyrocketed-amid-covid-19.
[12] Wolf, C. D. (2024, October 4). Cargo theft experts warn of peak season fraud. Transport Topics. https://www.ttnews.com/articles/cargo-theft-season.

Some OTGs are so vast and sophisticated that they have established their own call centers to manage their illegal supply chains. In many cases, these groups also operate seemingly legitimate warehouses and online marketplaces to store and sell stolen goods. In these scenarios, stolen goods are often exported out of the United States, repackaged, and then sold, sometimes for more than market value. A good example of this would be energy drinks. Certain energy drinks sold in the U.S. are banned in other countries, so thieves take advantage of the strong demand and sell the stolen drinks at an incredible mark-up in those foreign markets. Additionally, these types of products are usually seen as low-risk and high-value since they are easy to move and have high resale potential.

There are several factors and trends that are responsible for this uptick in frequency and sophistication of freight fraud. First, the COVID-19 global pandemic offered criminals a prime opportunity to exploit the vulnerabilities caused by a supply chain thrown into chaos by dramatic shifts in global supply and demand. Second, the digitization of domestic and international supply chains has created new vulnerabilities and thus opportunities for OTGs to exploit gaps using sophisticated and ever-evolving cyber capabilities. These groups can steal freight remotely by exploiting the technology that has been embedded into supply chains to move cargo more efficiently. Third, the erosion of traditional in-person direct business transactions—a past staple of traditional supply chain relationships—has created further opportunities for exploitation. Doing business with unknown companies and drivers has become normalized given that more shipments are now brokered via load boards and online platforms. This has made it relatively easy for the criminals to pose as legitimate brokers or carriers and fraudulently engage in business transactions with unwitting supply chain partners. Finally, the lack of coordinated investigations and prosecutions has emboldened these actions. Thieves have quickly realized that federal, state, and local law enforcement do not have the resources to stop them nor the interest to pursue sweeping investigations.

Many U.S. motor carriers are expending significant capital to protect themselves against these crimes, but obviously not all companies have the resources to do so. Several companies offer vetting services to motor carriers and brokers, but those services, while highly effective, come with an added cost. So, many in the trucking industry are often victims in one of two ways: either they lose significant sums of money through stolen freight, or they have to spend significant sums of money for services and advanced security measures to mitigate risk. With the speed at which our supply chain and cyber technologies are evolving, it costs more and more to fortify our businesses. Success in the transportation industry is no longer simply a matter of having the best drivers and the right equipment; motor carriers must now invest immense resources to have the strongest IT systems and the most diligent security personnel. In today's trucking environment, a strong defense is necessary for survival.

Commonly Targeted Freight

In general, thieves and fraudsters target goods that they can steal and sell quickly. This means that lower-value shipments, which are presumably less secure, are very attractive to cargo thieves. Accordingly, food and beverage items are targeted frequently and were the most commonly stolen type of freight in 2024.[13] Thieves prefer food and beverage products because there is consistently high demand, law enforcement typically does not initiate investigations of perishable goods quickly, and it is nearly impossible to track these items after they have been stolen.

[13] Verisk CargoNet. (2025, January 21). 2024 supply chain risk trends analysis. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-theft-trends/.

Furthermore, thieves and OTGs are always adapting to their environment and changing their tactics to reduce risk and maximize profit. As soon as the trucking industry, our supply chain partners, and law enforcement agencies identify theft trends and patterns, the criminals have already pivoted to new tactics and new targets that are presumably less secure. The trends of targeted commodities thus reflect the state of the market and transportation security at any given time. For example, during the COVID-19 pandemic, thieves targeted shipments of medical supplies and household supplies.[14] Due to the ongoing outbreaks of highly pathogenic avian influenza (HPAI) and the related egg shortage, approximately 100,000 eggs were stolen from a semi-trailer in Pennsylvania earlier this month.[15] Thieves are very perceptive to market conditions and will adjust their criminal schemes to capitalize on consumer demand.

Recent Examples of Cargo Theft in the News

- The U.S. Attorney's Office for the Northern District of Georgia announced that four men have been sentenced to prison for multiple cargo thefts of electronics, copper, and apparel throughout the Southeastern United States totaling more than $1.7 million. The stolen goods were then taken to Florida and sold. The case was investigated by the Federal Bureau of Investigation (FBI) with assistance from the Miami-Dade County Police Department, Economic Crime Bureau, and the FBI Miami Field Office.[16]
- The Tulare County Sheriff's Office in Central California linked Mexican cartels to a $2.25 million theft of heavy agricultural equipment and machinery. The individuals arrested face charges of grand theft, conspiracy, and receiving stolen property. A deputy district attorney says the maximum sentence would be three years behind bars.[17]
- The U.S. Attorney's Office for the Northern District of Illinois announced the indictment of a Lithuanian national for stealing over $9.5 million in goods in the Chicago area. He allegedly exploited vulnerabilities in a federal motor carrier registration system to obtain fictitious names, truck carriers, and brokers. He would then use these aliases to divert freight deliveries to alternate warehouses where he would then steal them.[18]
- The New Jersey State Police arrested four men from Philadelphia in a sting called "Operation Beef Bandit." The organized cargo theft ring broke into parked trailers at service areas while drivers were sleeping and stole "high-value goods" such as meat, alcohol, and seafood. The men are facing numerous charges, including receiving stolen property, possession of burglary tools, conspiracy to commit cargo theft, and criminal mischief.[19]

---

[14] Wolf, C. D. (2021, June 10). Truck cargo thefts skyrocketed amid COVID-19. Transport Topics. https://www.ttnews.com/articles/truck-cargo-thefts-skyrocketed-amid-covid-19.

[15] Hume, J. (2025, February 14). 100,000 eggs stolen: Breaking news or an old cargo theft trend? FleetOwner. https://www.fleetowner.com/safety/article/55267606/egg-heist-highlights-food-and-beverage-cargo-theft-risks-but-is-it-a-trend.

[16] U.S. Attorney's Office, Northern District of Georgia. (2024, June 26). Members of a Cargo Theft Ring Sentenced to Prison. https://www.justice.gov/usao-ndga/pr/members-cargo-theft-ring-sentenced-prison.

[17] Rodriguez, Rich. (2024, October 29). Sheriff links Mexican cartels to $2.25 million theft of Central California farm equipment. abc3340. https://abc3340.com/news/nation-world/sheriff-links-mexican-cartels-to-225-million-theft-of-central-california-farm-equipment.

[18] U.S. Attorney's Office, Northern District of Illinois. (2024, June 7). Suburban Chicago Man Charged in Federal Court With Stealing More Than $9.5 Million in Interstate Shipments. https://www.justice.gov/usao-ndil/pr/suburban-chicago-man-charged-federal-court-stealing-more-95-million-interstate#:~:text=The%20indictment%20alleges%20that%20Zigmantas,of%20theft%20of%20interstate%20shipments.

[19] Hartman, Trish. (2024, September 17). 4 Philadelphia men arrested in 'Operation Beef Bandit' in connection to organized cargo theft ring. 6abc. https://6abc.com/post/4-men-philadelphia-arrested-operation-beef-bandit-connection-organized-cargo-theft-ring-tri-state/15314427/.

- The California Highway Patrol (CHP) announced that a monthslong multi-agency investigation into a cargo and vehicle theft operation in Southern California yielded more than 50 arrests, hundreds of thousands in U.S. currency, and over $8 million in stolen cargo. During the investigation, investigators also recovered 425 pounds of methamphetamine, 48 gallons of liquid methamphetamine, a clandestine methamphetamine lab, 20 rifles and handguns, and 20 stolen vehicles.[20]
- The U.S. Attorney's Office for the District of New Jersey announced that three men pleaded guilty to their roles in a conspiracy to burglarize approximately 55 United Parcel Service warehouses across the United States, resulting in the theft of over $1.6 million worth of merchandise. The men sought parcels marked with "lithium-ion battery" warnings, which indicated that the packages contained high-value electronic devices such as cell phones.[21]
- The Grapevine Police Department uncovered a multimillion-dollar cargo theft ring and charged seven suspects with engaging in organized criminal activity. The theft ring was responsible for burglaries of electronics and high-value merchandise totaling more than $10 million in five cities: Grapevine, Plano, Fort Worth, Coppell, and Dallas.[22]
- CHP's Organized Retail Crime Task Force and Cargo Theft Interdiction Program conducted a statewide enforcement operation called "Operation Overloaded," which targeted individuals involved in a cargo theft scheme believed to have stolen over $150 million worth of goods from more than 200 cargo loads. CHP arrested 40 people during the operation and seized over $50 million worth of stolen merchandise and 20 stolen cargo trailers. The authorities also confiscated several vehicles, multiple firearms (including ghost guns), over $550,000 in cash, and 13 gold bars. The suspects involved in the theft scheme face several felony charges, including conspiracy to commit grand theft, grand theft of cargo, vehicle theft, and identity theft.[23]
- The U.S. Attorney's Office for the Southern District of Florida announced that the final member of a cargo theft ring had been convicted of stealing 19,000 pounds of Perry Ellis perfume worth over $230,000. The shipment was destined for Laredo, Texas, but 22 of the 24 pallets of perfume never left Hialeah, Florida, because of the theft.[24]
- The Kentucky State Police announced that its Vehicle Investigations Branch had ended a year-and-a-half-long investigation into an organized theft ring allegedly responsible for around $10 million in stolen freight. During the investigation, the Kentucky State Police opened 16 cargo theft investigations, resulting in 10 federal indictments and seven arrests. Investigators had noted a rise in stolen freight throughout the state that specifically targeted the food and beverage industry, as well as an increase in incidents of copper theft.[25]

---

[20] DuBose, Josh. (2024, June 27). Cargo theft sting nets $325K in cash, $8M in stolen goods and 51 arrests. KTLA5. https://ktla.com/news/local-news/cargo-theft-sting-nets-325k-in-cash-8m-in-stolen-goods-and-51-arrests/.

[21] U.S. Attorney's Office, District of New Jersey. (2024, March 28). Three Philadelphia Men Admit Roles in Conspiracy to Burglarize United Parcel Service Warehouses Across United States, Stealing over $1.6 Million in Packages. https://www.justice.gov/usao-nj/pr/three-philadelphia-men-admit-roles-conspiracy-burglarize-united-parcel-service.

[22] Myers, Doug and J.D. Miles, S.E. Jenkins. (2024, November 19). 7 charged with organized criminal activity in multimillion-dollar North Texas cargo theft ring. CBS News. https://www.cbsnews.com/texas/news/seven-charged-in-north-texas-multimillion-dollar-cargo-theft-ring-bust/.

[23] FCCR (2023, May 8). 40 Individuals Linked to $150 Million Cargo Theft Scheme Arrested. https://fccr.co/40-individuals-linked-to-150-million-cargo-theft-scheme-arrested/?srsltid=AfmBOoon6CFDIDj0SvU-QR5A5c8VLS0Mq-pjEZgqOYJG3_PKvopVrzdl.

[24] U.S. Attorney's Office, Southern District of Florida. (2024, January 31). Final Member of Cargo Theft Ring Convicted of Stealing 19,000 Pounds of Perry Ellis Perfume Worth Over $230,000. https://www.justice.gov/usao-sdfl/pr/final-member-cargo-theft-ring-convicted-stealing-19000-pounds-perry-ellis-perfume.

[25] Witkowski, Ryan. (2023, December 22). Cargo theft investigators recover over $5M in stolen property. Landline. https://landline.media/cargo-theft-investigators-recover-over-5-million-in-stolen-property/.

- The U.S. Attorney's Office for the Middle District of Florida announced that four men have pleaded guilty to charges involving cargo theft of an interstate shipment of goods and receipt and possession of stolen goods. The men stole a tractor trailer containing $500,000 worth of Patron tequila that was parked near U.S. Route 301 in Tampa. The tequila was an interstate shipment from Texas that was enroute to a business in Lakeland, Florida.[26]
- The U.S. District Court for the Central District of California issued a final judgment against a moving company for repeated unauthorized transportation of household goods, in violation of FMCSA's registration requirements, and ordered to pay $25,000 in fines.[27]

Challenges With Understanding the Scope of Freight Fraud:

Because fraud and cargo theft within our supply chains are increasing at such an alarming rate, it is difficult to aggregate data that accurately represents the current breadth and scope of this problem.

Underreporting of Cargo Theft and Poor Data

Cargo theft is severely underreported in crime statistics. The FBI's Universal Crime Reporting program attempts to generate reliable statistics on cargo theft, but the most recent report was published in 2019, and local agencies are under no obligation to report. Additionally, industry reporting of cargo theft is not mandatory. The utilization of voluntary data on cargo theft from law enforcement and industry certainly understates the scope and value of cargo theft.

Importantly, freight fraud and cargo theft are regularly underreported by industry because transportation companies fear publicity that could damage their business reputations. They do not want to be perceived by clients or competitors as having weak security or poor management, which would risk customer relationships and future business growth opportunities.

Another factor contributing to industry underreporting is general confusion about appropriate reporting protocols. Motor carriers and brokers may not know the correct jurisdiction to which the crime should be reported because they may not know where or when exactly the theft took place. There are also situations when victims may reach out to law enforcement to report a crime and seek assistance for cases of fraud or theft, but rather than assistance, they are met with confusion and dismissiveness. Often, when trucking companies attempt to file a report with local and state law enforcement agencies, they are told to file a claim with their insurance company instead. This happens usually because local and state law enforcement officers often do not have the necessary training to recognize that cargo theft is not simply a property crime. Alternatively, law enforcement officers will note jurisdictional issues given the interstate nature of the crime and direct motor carriers to report elsewhere. Importantly, it should be noted that, for many motor carriers and logistics companies, it does not make financial sense to file theft claims with insurance because the value of the stolen freight is often less than their deductible.

Cargo theft is misunderstood for many reasons. First, the law that criminalizes cargo theft at the federal level never mentions or defines the term, "cargo theft."[28] Furthermore, the state statutes defining and criminalizing cargo theft and other types of freight fraud are different for each state. As highlighted in a recent report from the Federal Maritime Commission (FMC), this inconsistency creates a lot of

[26] U.S. Attorney's Office, Middle District of Florida. (2020, October 29). Four Individuals Plead Guilty In Tequila Cargo Theft Ring. https://www.justice.gov/usao-mdfl/pr/four-individuals-plead-guilty-tequila-cargo-theft-ring.
[27] Federal Motor Carrier Safety Administration (2024, December 6). FMCSA Wins Landmark Judgement Against Moving Company. https://www.fmcsa.dot.gov/newsroom/fmcsa-wins-landmark-judgement-against-moving-company.
[28] 18 U.S.C. § 659

confusion for law enforcement, especially since these crimes usually involve bad actors who cross state lines.[29] It is not always clear which crimes constitute cargo theft and which agencies have the authorities to investigate and prosecute these offences. Jurisdictional confusion leads to ineffective enforcement of applicable cargo theft laws, and the absence of criminal investigations and prosecutions emboldens criminals to continue their illegal activities.

Fundamental misunderstandings about cargo theft among law enforcement officers, especially at the state and local levels, are not simply the result of negligent policing. Shifting priorities and the loss of dedicated funding means that law enforcement officers are not properly equipped to address this dynamic and complex issue. The sharp decline of experienced cargo theft investigators at state and local levels has been a common trend over the past several years. For example, the State of Georgia previously had a state-wide, leading-edge frontline task force dedicated to investigating cargo thefts. But in 2018, the task force was disbanded due to a lack of support from the state government.[30]

Current Cargo Theft Data

With the prevalence of underreporting in mind, there are groups that have attempted to estimate the impact of these types of crimes. One such organization is CargoNet, which is a subscription-based information-sharing network that collects data about instances of cargo theft that are voluntarily submitted by companies, law enforcement, and other sources. In 2024, 3,625 theft incidents were reported to CargoNet, a 27% increase compared to the previous year. It is believed that this figure represents only a small percentage of the total thefts committed. In 2024, CargoNet estimated the total loss to industry at more than $450 million. Per incident, the estimated average value stolen was $202,364, up from $187,895 in 2023.[31]

Overhaul, another company that provides various services in the cargo theft mitigation space, publishes a report annually that details significant theft incidents in the United States and Canada. According to their most recent annual report, Overhaul recorded a total of 2,217 cargo thefts throughout the United States in 2024. These numbers represent a 49% increase in volume and a 17% increase in average value when compared to 2023.[32]

Companies like CargoNet and Overhaul are publishing data based on the incidents that are reported, but as previously stated, cargo theft is notoriously underreported. With that in mind, we are of the opinion that the problem is even bigger than what these organizations' data show. And we are not alone. NICB,[33]

[29] Bentzel, C. W. (2024, December). Cargo theft: Evaluation of the challenge of combatting cargo theft with recommendations on how to reduce the impact of cargo theft. Federal Maritime Commission. https://news.tianet.org/wp-content/uploads/sites/3/2024/12/2024.12-FMC-Bentzel-Cargo-Theft-Report.pdf

[30] Lockridge, D. (2025, February 20). Cargo theft likely to spike over the next seven days. Commercial Carrier Journal. https://www.ccjdigital.com/workforce/safety/article/15281505/cargo-theft-likely-to-spike-over-the-next-seven-days.

[31] Verisk CargoNet. (2025, January 21). 2024 supply chain risk trends analysis. CargoNet. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-theft-trends/.

[32] Overhaul (2025, January). United States & Canada: Annual Cargo Theft Report 2024. https://over-haul.com/wp-content/uploads/2025/02/US-and-Canada-Annual-Cargo-Theft-Report-2024.pdf.

[33] National Insurance Crime Bureau. (2024, November 15). The rise of cargo theft: A billion-dollar industry. NICB. https://www.nicb.org/news/blog/rise-cargo-theft-billion-dollar-industry.

Homeland Security Investigations (HSI)[34], and the FBI[35] have all estimated that cargo theft in the United States is a $15 to $35 billion industry.

Barriers to Investigation and Prosecution:

ATA has been engaging with representatives from the FBI, the Department of Justice (DOJ), HSI, and USDOT. While these agencies know cargo theft is a significant problem in the U.S., often they lack the resources to make a dent in the problem.

State and local authorities could better help these federal agencies by identifying and demonstrating links between various cargo theft cases in order to connect seemingly isolated thefts to an OTG. Establishing connections between multiple theft incidents will enable federal authorities to take prosecutorial action, since the standard for federal involvement is much higher. In order for DOJ to even consider prosecuting a cargo theft case, the value of the goods stolen must total at least $1.5 million, according to the United States Sentencing Commission.[36] This threshold can be met in two ways: either a single theft incident totals at least $1.5 million in losses, or multiple related theft incidents (potentially targeting multiple victims) total at least $1.5 million in losses.

Given that the estimated average value per theft in 2024 was $202,364,[37] it is imperative that state and local law enforcement better track incidents of cargo theft because most single incidents do not reach the monetary threshold to warrant federal involvement. When dots are connected, DOJ can become involved, thieves can be prosecuted, and victims can receive justice. If law enforcement identifies a link (i.e. a single OTG stealing multiple trailers) DOJ will have the green light to utilize more resources and dedicate more manpower to bringing these criminals to justice. Additionally, more prosecutions will serve as a deterrent, and hefty sentences will hopefully make potential offenders aware of the consequences of their actions.

One of the major reasons why it can be difficult for law enforcement agencies to connect individual theft cases is due to the inconsistency in the statutory definition of cargo theft across jurisdictions. As previously mentioned, statutes defining and criminalizing cargo theft are different for each state. Additionally, the law that criminalizes cargo theft at the federal level never mentions or defines the term, "cargo theft."[38] These differences create confusion and make is difficult for investigators and prosecutors to combine efforts to combat cargo theft. Given that these crimes usually involve freight that crosses state lines, questions of jurisdictional authority regularly arise. Relatedly, as mentioned in the FMC report,[39] definitional differences often result in a struggle to form a unified assessment of offenses and to use the assessment to coordinate law enforcement response. Overall, jurisdictional confusion leads to ineffective enforcement of applicable cargo theft laws, and the absence of criminal investigations emboldens criminals to continue their illegal activities.

---

[34] U.S. Immigration and Customs Enforcement. Operation Boiling Point. https://www.ice.gov/about-ice/hsi/news/hsi-insider/op-boiling-point.
[35] Josephs, L. (2023, March 25). Cargo theft led by food and beverage is surging across the U.S. CNBC. https://www.cnbc.com/2023/03/25/cargo-theft-led-by-food-and-beverage-is-surging-across-the-us.html.
[36] U.S.S.C, §2B1.1
[37] Verisk CargoNet. (2025, January 21). 2024 supply chain risk trends analysis. CargoNet. https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-theft-trends/.
[38] 18 U.S.C. § 659
[39] Bentzel, C. W. (2024, December). Cargo theft: Evaluation of the challenge of combatting cargo theft with recommendations on how to reduce the impact of cargo theft. Federal Maritime Commission. https://news.tianet.org/wp-content/uploads/sites/3/2024/12/2024.12-FMC-Bentzel-Cargo-Theft-Report.pdf

How Congress Can Help Combat Freight Fraud and Safeguard U.S. Supply Chains:

Economic security is national security, and the unfortunate reality is that our national security has been compromised because OTGs and TCOs have successfully infiltrated our domestic supply chains and exploited enforcement gaps in the stream of interstate commerce. The trucking industry and U.S. supply chains are both interstate by nature—goods cross state lines and move through ports of entry nearly every second of every day—which is why ATA and our supply chain partners are urging a federal response to the alarming rise of freight fraud across the country. OTGs have identified the glaring gaps between local, state, and federal law enforcement regimes as low-risk, high-reward opportunities to build out sophisticated fraud and theft schemes and remain undetected. OTGs are exploiting U.S. transportation and distribution networks with impunity because there is no concerted effort from the federal government to investigate and prosecute. And without those critical deterrence factors, criminals will continue to infiltrate our supply chains, profit off the vulnerability of American businesses, and fund other illicit enterprises with the money generated from fraud and theft schemes. The costs of inaction are enormous, both in terms of financial losses and the denigration of national security.

Therefore, we urge Congress to embrace its responsibilities pursuant to the Commerce Clause of the U.S. Constitution and leverage the cross-cutting enforcement capabilities of the federal government to help combat rampant supply chain fraud and theft. We are grateful to Senators Fischer and Duckworth for tackling the issue of fraud in the moving and storage industry by introducing the *Household Goods Shipping Consumer Protection Act* (S. 337). This legislation provides FMCSA with the necessary tools, resources, and authorities to protect consumers from fraud, while also helping small businesses in the household goods shipping industry protect their businesses and reputations. The *Household Goods Shipping Consumer Protection Act* will help prevent bad actors from preying on individuals and families during stressful relocation events.

Specifically, this bill restores FMCSA's ability to impose civil penalties against unauthorized brokers and other bad actors, allowing the agency to act swiftly in meting out penalties. The bill also requires companies operating in the household goods sector to maintain a legitimate place of business. Too often, consumers fall victim to scammers who set up freight businesses that exist only on paper and who have no sincere intention of helping them move. The *Household Goods Shipping Consumer Protection Act* gives states the ability to use federal funds to enforce consumer protection laws and root out fraudulent actors before they strike. This bipartisan legislation is a critical element of a broader federal response to freight fraud, and we hope that Congress advances it expeditiously.

We hope that this Committee will take further action to help combat freight fraud by supporting the *Safeguarding Our Supply Chains Act* (H.R. 8834 from the 118th Congress). The robust coalition of stakeholder support for the *Safeguarding Our Supply Chains Act* is a testament to the breadth and scope of U.S. industries that are impacted by supply chain fraud and theft. No industry wants to be seen as the target of criminal activity, but the situation has become so dire that the American Trucking Associations, along with the Association of American Railroads, the National Association of Manufacturers, the National Milk Producers Federation, the National Retail Federation, NATSO, the Retail Industry Leaders Association, the Transportation Intermediaries Association, the U.S. Chamber of Commerce, the U.S. Dairy Export Council, and the World Shipping Council have all joined together in advocating for federal intervention through the *Safeguarding Our Supply Chains Act*.

The legislation directs HSI, in conjunction with the Attorney General and the FBI, to establish a federal task force to prevent and reduce organized crime throughout all stages of the supply chain—including production, transportation, freight brokerage, processing, storage, distribution, and retail—as well as

detect, disrupt, and deter OTGs and individuals that are targeting all stages of the supply chain. The legislation also directs HSI to establish a coordination center to collect and analyze data related to fraud and theft at all stages of the supply chain and identify regions in the United States, modes of transportation, distribution networks, and retail stores that are experiencing high volumes of organized crime. The intelligence generated by the coordination center will inform the personnel and resource allocations of the task force to ensure a dynamic and efficient response to evolving criminal tactics.

This legislation was modeled after the *Jaime Zapata Border Enforcement Security Task Force Act*, which was signed into law by President Obama in 2012. This law established the Border Enforcement Security Task Force (BEST) within the Department of Homeland Security (DHS) and is a premier example of successful collaboration between federal, state, local, tribal, and foreign law enforcement agencies to execute coordinated activities in furtherance of national security objectives. The task force established by the *Safeguarding Our Supply Chains Act* mirrors the BEST's highly successful framework to similarly incentivize collaboration between law enforcement agencies. Because of the interstate nature of supply chain fraud and theft and its relation to organized conspiracy, the federal government must take a leadership role in coordinating enforcement activities and connecting the dots. Moreover, given HSI's unique cross-border authorities and trade expertise, the FBI's role as the lead federal agency in enforcing the federal law on cargo theft (18 U.S.C. §659), and FMCSA's exclusive authority to challenge fraudulent broker licensing, it is imperative that the federal government harmonize its disparate functions to address the gaps in our supply chain that are currently being exploited.

Congress should also consider opportunities to address supply chain fraud and theft through the appropriations process. The FY2025 Homeland Security Appropriations bill as passed by the House of Representatives directs Homeland Security Investigations (HSI) to establish a Supply Chain Fraud and Theft Task Force and provides $2 million to fund the initiative. The FY2025 Commerce, Justice, Science, and Related Agencies Appropriations bill as reported by the House Committee on Appropriations directs DOJ to allocate no less than $2 million for the purpose of prosecuting crimes involving cargo theft and instructs several United States Attorneys' Offices to assign at least one attorney to prioritize cargo theft prosecutions. The FY2025 Transportation, Housing and Urban Development Appropriations bill as passed by the Senate Appropriations Committee also directs a coordinated effort from the USDOT, DOJ, DHS's Supply Chain and Resilience Center, and relevant stakeholders to confront the issue of cargo theft.

Additionally, we encourage this Committee to oversee and support the critical work already underway at the FMCSA to address registration fraud and facilitate a smooth transition to the newly modernized and enhanced FMCSA Registration System.

Passage of the *Household Goods Shipping Consumer Protection Act* and the *Safeguarding Our Supply Chains Act*, Congressional oversight of FMCSA's transition to the new system, and enactment of key appropriations provisions that direct funding and federal attention to the growing threat of organized supply chain crime are vital to our nation's economic security.

In Conclusion:

Chairman Young, Ranking Member Peters and members of the subcommittee, thank you again for the opportunity to testify before you today on behalf of the American Trucking Associations. Supply chain fraud and cargo theft are imperiling the trucking and supply chain logistics industry. My companies, Tanager Logistics and Double Diamond Transport, have experienced these threats first-hand, and we

have been forced to navigate a complex and often ineffective response from varying law enforcement agencies and federal regulators. My peers in Texas, across the nation, and up and down the supply chain are confronting similar challenges. These challenges are sophisticated and are disrupting the supply chain, harming the economy, and ultimately, hitting the consumer.

It is imperative that action is taken at the federal, state, and local levels to confront and neutralize this growing threat. We need more cooperation and interagency information-sharing, as well as a more robust investigative and prosecutorial posture, to tackle these challenges head-on. Importantly, we need a commitment from Congress to provide the tools and resources necessary to facilitate that unified response.

The trucking and supply chain logistics industry stands ready to collaborate with every stakeholder committed to halting the rise of supply chain fraud and cargo theft, and we welcome the opportunity to work with this subcommittee, Congress, and the new Administration in that effort. Thank you for your attention and leadership in holding today's hearing. We look forward to a continued dialogue.