Statement of

THE HONORABLE DAVID J. GLAWE

PRESIDENT AND CHIEF EXECUTIVE OFFICER

NATIONAL INSURANCE CRIME BUREAU

Before the U.S. Senate Committee on the Judiciary

For a Hearing on:

"Beyond the Smash and Grab: Criminal Networks and Organized Theft"

July 15, 2025

I. Introduction

Chairman Grassley, Ranking Member Durbin, and Members of the Committee:

Thank you for the invitation to testify on behalf of the National Insurance Crime Bureau (NICB), and for holding this important hearing on organized retail and cargo theft—a complex and rapidly growing threat to American consumers and job creators, as well as to our national security.

I am the President and Chief Executive Officer of NICB. Headquartered in Oak Brook, Illinois, NICB has been fighting insurance-related crime and organized theft since 1912, dating back to our inception as the Automobile Protective and Information Bureau; transformation into the National Automobile Theft Bureau in 1927; and our consolidation in 1992 as the National Insurance Crime Bureau.

NICB maintains operations in every state around the country. Over the many years of our existence and through the experience and lengthy tenure of many of our agents, NICB has cultivated strong partnerships and trusted relationships with federal, state, and local agencies across the nation in support of our member carriers. Our employees work hand-in-hand on a daily basis with those agencies to provide assistance in all manner of cases, including on the frontlines of combating cargo theft. NICB's special agents and intelligence analysts support our local, state, and federal law enforcement partners in identifying, investigating, and prosecuting cargo theft rings—as well as in theft recoveries.

But these highly sophisticated criminals are gaining the upper hand. What NICB sees in the field is nothing short of a call to action—

• In 2024, cargo crimes increased to a historic high—up 27% from 2023—and are expected to rise another 22% by the end of this year.

- Criminal networks are exploiting supply chain vulnerabilities and increasingly employing identity theft and fraudulent cargo pickups, posing as fictitious carriers, and using other cyber-enabled logistics manipulation to achieve their objectives.
- Once secured, stolen goods—everything from sports drinks to sports cars—are routinely routed out of our country and into black markets and the hands of transnational criminal organizations to finance other illicit activities, including drug and weapons trafficking and even terrorism.

These highly orchestrated theft rings are not just targeting our nation's major ports or urban centers. They operate in our small towns, along rural highways, and on remote rail corridors. The impacts, including increased costs, are felt from Main Street to Wall Street.

Now is the time for both the public and private sectors to work together to stop criminal organizations from stealing from the real victims: American consumers and their communities.

Congress can help in several ways, including through passage of the bipartisan Combating Organized Retail Crime Act (CORCA). This bill would strengthen deterrence and collaboration keys to securing our supply chains, disrupting transnational criminal networks, and keeping costs down for all Americans.

II. NICB Background

With an over 110-year history, NICB is the nation's premier non-profit organization exclusively dedicated to detecting, preventing, and deterring insurance fraud and insurance-related crimes through intelligence-driven operations.

We are supported by approximately 1,200 property and casualty insurance companies, associate members, and other strategic partners within the anti-fraud and anti-crime ecosystem. Many of our members underwrite America's supply chains and retailers, including those most impacted by organized theft. While we provide value to our members and law enforcement—such as through on-the-ground investigative support; intelligence reporting and information sharing; education and training; and advocacy on public policy matters—NICB also serves a significant public benefit by helping to stem the estimated billions of dollars in economic harm that insurance-related crime causes every year to consumers and policyholders nationwide.

Insurance fraud is not a victimless crime. According to the Federal Bureau of Investigation (FBI), insurance fraud (excluding health insurance) is estimated to be more than \$40 billion per year, costing the average U.S. family between \$400 and \$700 annually in the form of increased

premiums.¹ The Coalition Against Insurance Fraud estimates that the damage is far greater, with fraudsters stealing approximately \$308 billion each year from American consumers.² These crimes are complex and can take many forms—from vehicle and cargo theft; staged accidents and slip-and-fall schemes; and home and auto repair scams; to identity theft, predatory towing, and medical billing fraud—and are limited only by the scope of fraudsters' capabilities and resourcefulness.

To disrupt and deter these crimes, NICB sits at the intersection of the insurance industry, insurance regulators, and law enforcement across the country. This ecosystem recognized long ago that communication and collaboration is key to the fight against insurance crime and to protect consumers.

We know that criminals and fraudsters are coordinated—often within sophisticated, organized networks—and thus we should be too. To encourage that coordination, most states mandate that insurers report suspected insurance fraud and related crimes to the appropriate Department of Insurance, state insurance fraud bureau, or law enforcement agency. NICB has long served as a facilitator of these reports. In fact, we are codified by name into many states' reporting statutes and regulations. In nearly all 50 states, insurers can report suspected insurance crimes and thefts directly to NICB. In partnership with state insurance commissioners, NICB relays these reports to the appropriate state authority.

This process provides NICB with unique, unmatched visibility into organized crime and theft trends nationwide that directly target or impact the insurance industry. Our expert analysts can identify trends and patterns—and can uncover complex criminal networks—that are visible only from NICB's multi-state, multi-carrier vantage point. NICB shares this vital information to our members and other strategic partners—through intelligence reports and actionable insights—to alert them of potentially overlapping networks of insurance fraudsters.³

In 2024 alone, NICB received over 180,000 reports from insurers about suspicious activity and fraud connected to policies they underwrite. Through these reports and related sources, NICB identified over 1,600 organized crime rings and issued over 2,200 alerts to our members and partners.⁴

Equipped with this unique visibility, NICB personnel-many of whom are themselves former law enforcement-work every day with our federal, state, and local law enforcement

¹ Insurance Fraud, Federal Bureau of Investigation, *available at* <u>https://www.fbi.gov/stats-services/publications/insurance-fraud</u>.

² Fraud Stats, Coalition Against Insurance Fraud, available at <u>https://insurancefraud.org/fraud-stats/</u>.

³ See, e.g., New York Lawyers And Doctor Sentenced For Defrauding New York City-Area Businesses And Their Insurance Companies Of More Than \$31 Million Through Massive Trip-And-Fall Fraud Scheme, U.S. Attorney's Office for the Southern District of New York (April 25, 2023) (U.S. Attorney "thank[ing] the National Insurance Crime Bureau for their assistance in the investigation") available at https://www.justice.gov/usao-sdny/pr/new-york-lawyers-and-doctor-sentenced-defrauding-new-york-city-area-businesses-and.

⁴ NICB Annual Report 2024, *available at <u>https://www.nicb.org/annual-reports/2024</u>.*

partners to assist in the investigation and prosecution of crimes affecting not only the insurance industry but our broader community. At the federal level, NICB is especially proud of our longstanding partnerships with the U.S. Department of Homeland Security (DHS) and the FBI. For decades, NICB has served to facilitate information sharing between the government and private industry in our joint mission to defeat fraudsters, and that work continues today in our collaborative efforts to combat criminal threats that transcend state and national borders.

In fact, NICB's unique expertise and collaboration with our federal partners has helped solve some of the most devastating terrorist attacks and vehicle-related crimes on U.S. soil. For example:

- NICB special agents, using Vehicle Identification Number (VIN) and related information within NICB databases, helped identify the vehicle used in the February 26, 1993, World Trade Center bombing, ultimately leading to the arrest and prosecution of the vehicle's renter and his co-conspirators.
- In the aftermath of the April 19, 1995, Oklahoma City bombing, which killed 168 people, the FBI called NICB to assist in identifying the vehicle used in the bombing. Using NICB-developed technology and multi-state vehicle and insurance records, agents reconstructed the VIN, which led to the identification of the Ryder truck that carried the bomb and ultimately the identification of Timothy McVeigh and his coconspirator, Terry Nichols.
- Following the 2020 Nashville Christmas bombing, which damaged 65 buildings and displaced dozens of businesses and residents, the FBI called NICB for help in identifying the suspect vehicle. NICB special agents provided analysis and advice to the FBI, including in terms of identifying and prioritizing what vehicle parts were critical to recover. Authorities ultimately identified the vehicle and its owner through information provided by NICB.

Today, as crimes continue to evolve with technology, stronger collaboration is more critical than ever. This is especially true in combatting organized retail and cargo theft.

III. NICB's Expertise and Role in Combating Cargo Theft

Cargo theft is big business, driven by big opportunity. In recent years, sophisticated criminal networks have increasingly engaged in brazen theft of cargo moving through our nation's supply chains. They have even infiltrated segments of the shipping industry, exploiting technology vulnerabilities to impersonate legitimate links in the supply chain including trucking companies.

Unfortunately, these crimes are on the rise. In 2024, cargo theft losses increased to an alltime high, up 27% from 2023.⁵ Losses are predicted to rise another 22% from already historic levels by the end of 2025.

In 2023, the value of stolen merchandise and estimated loss rose to more than \$1 billion, with the average value of an individual cargo theft topping \$202,000. Other estimates suggest that total cargo losses may, in fact, reach up to \$35 billion annually.⁶

Since 2022, NICB has opened an average of 150 cargo crime cases per year. And in the last 18 months, NICB assisted in more than 240 cargo theft investigations, leading to more than 70 recoveries valued at nearly \$40 million.

From NICB's vantage point, most cargo thefts are <u>not</u> the result of small operations seeking quick payouts. Rather, cargo theft is most often orchestrated by well-funded, sophisticated criminal organizations—including Transnational Criminal Organizations (TCO) like the Armenian Mafia⁷ and Sinaloa cartel,⁸ as well as operations out of China and Eastern Europe.⁹ These complex operations and resale networks span multiple states and countries.

For example, NICB recently assisted law enforcement in uncovering a sophisticated international criminal enterprise which utilized multiple business email compromises to successfully arrange and ultimately export stolen industrial equipment for resale overseas. This investigation is ongoing. This criminal enterprise largely conducted its operations from overseas by using business email compromises and Voice over Internet Protocols to deceive legitimate suppliers, freight brokers, and transporters.

In 2024, NICB special agents assisted an investigation across Southern California and Arizona that resulted in the arrest of more than 50 individuals, and the recovery of vehicles, weapons, drugs, currency, and more than \$8 million of cargo stolen from the Burlington Northern Santa Fe Railway line.¹⁰

⁵ "2024 Supply Chain Risk Trends Analysis," Verisk CargoNet (Jan. 21, 2025) *available at* <u>https://www.cargonet.com/news-and-events/cargonet-in-the-media/2024-theft-trends/</u>.

⁶ Operation Boiling Point, U.S. Immigration and Customs Enforcement (updated Feb. 8, 2025) available at <u>https://www.ice.gov/about-ice/hsi/news/hsi-insider/op-boiling-point</u>.

⁷ "13 'Armenian Mafia' members arrested in connection to murder, \$83M Amazon cargo theft," Courthouse News Service (May 20, 2025) *available at* <u>https://www.courthousenews.com/13-armenian-mafia-members-arrested-in-connection-to-murder-83m-amazon-cargo-theft/</u>.

⁸ "Grand theft cargo: Sinaloa cartel targets US rail companies," Border Report (June 5, 2025) *available at* <u>https://www.borderreport.com/immigration/border-crime/grand-theft-cargo-sinaloa-cartel-targets-us-rail-companies/</u>.

⁹ See "Cargo theft is a growing national security issue," Sen. Todd Young (R-IN), The Washington Times (June 24, 2025) available at <u>https://www.washingtontimes.com/news/2025/jun/24/cargo-theft-growing-national-security-issue/</u>.

¹⁰ NICB Cargo Crime Threat Assessment (June 5, 2025) at 10.

In 2023, NICB provided special operations support to a California Highway Patrol (CHP) cargo theft task force investigation of a railway burglary ring that resulted in more than 100 arrests.¹¹ In another California case, NICB worked with CHP and several other law enforcement agencies from the San Bernardino County Auto Theft Task Force resulting in the arrest of more than 50 individuals. Law enforcement executed search warrants yielding hundreds of thousands of dollars and over \$8 million in stolen cargo.¹²

In one multi-state theft ring, employees at a Memphis, TN warehouse distribution center fraudulently used preprinted address labels to divert shipments of name brand shoes to a cohort who worked at a company warehouse on the West Coast, who would then sell the shoes on the streets of Los Angeles. To date, investigators have recovered \$5 million in stolen shoes.¹³

And recently, NICB assisted the U.S. Customs and Border Protection (CBP) Outbound Enforcement Team, California Highway Patrol Foreign Export and Recovery team, and the California Highway Patrol Cargo Theft Interdiction Program in the inspection and identification of stolen Vizio, LG and Samsung televisions that were being exported to Panama.

NICB's longstanding partnership with CBP has only further confirmed the international scope of cargo-related theft. Every day, in fact, our special agents assist CBP at major U.S. ports.

In September 2024, NICB and CBP announced our latest partnership, "Operation Terminus," to prevent stolen vehicles from being smuggled out of the country through cargo containers at seaports around the nation.¹⁴

Through this joint operation, NICB agents—working alongside CBP officers—have inspected shipping containers and discovered multiple high-end vehicles worth more than \$100,000 each, resulting in recoveries worth millions of dollars. These vehicle seizures are occurring at ports from New York, Newark, Norfolk, and Baltimore and south to Savannah and Miami.

Many of the recovered stolen vehicles were bound for several different countries in Africa.

Additionally, our joint operations recovered hundreds of rounds of various caliber ammunition that were concealed in vehicles destined for Nigeria and other African ports.

¹¹ Id.

¹² "Cargo theft sting nets \$325k in cash, \$8m in stolen goods and 51 arrests," KTLA-5 (June 27, 2024) *available at* <u>https://ktla.com/news/local-news/cargo-theft-sting-nets-325k-in-cash-8m-in-stolen-goods-and-51-arrests/</u>.

¹³ NICB Cargo Crime Threat Assessment (June 5, 2025) at 10.

¹⁴ "NICB Partners with U.S. Customs and Border Protection to Stop Export of Stolen Vehicles," National Insurance Crime Bureau (Sept. 5, 2024) *available at* <u>https://www.nicb.org/news/news-releases/nicb-partners-us-customs-and-border-protection-stop-export-stolen-vehicles</u>.

As with many forms of stolen goods and cargo, we know that exported stolen vehicles are often laundered or resold to support other illicit activities such drug and weapons smuggling, and even international terrorism.

IV. Complex Tactics Compel a Coordinated Response

The sheer volume of cargo in transit, combined with vulnerabilities at multiple points in the supply chain, presents private industry and law enforcement with a persistent and evolving threat landscape. While multiple factors may be contributing to the rise in (and profitability of) cargo thefts, NICB's investigations and analyses reveal that organized criminal networks are increasingly exploiting technology gaps to achieve their objectives.

For example, after stealing a shipment, many criminals will use GPS jamming devices to disrupt onboard tracking systems, thus allowing stolen cargo to be moved without detection. NICB special agents have confirmed confiscations of these devices in cargo theft incidents and noted that thieves frequently disable GPS trackers that are not concealed effectively.

Additionally, over the last few years, criminals have increasingly infiltrated the "for hire" shipping industry itself to engage in strategic cargo theft and fictitious pickups—often impersonating (or deceiving) legitimate transport companies and other sectors of the supply chain. To carry out this fraud, organized crime groups exploit technology to illegitimately obtain the valid registered Motor Carrier number of a retiring (and otherwise legitimate) transporter. This allows criminals to hide behind credible credentials in deceiving freight brokers. Once hired by an unwitting broker, the criminal group—masquerading as a legitimate transporter—acquires the load, then ceases communication to avoid detection, completing the theft.

In other scenarios, the criminal group may pose as a legitimate broker, only to have cargo such as vehicles or other valuable goods—re-routed mid-transit to the group's preferred destination.

NICB's federal law enforcement partners have witnessed criminal enterprises orchestrate these types of cargo crimes from overseas, deceiving one or more key links in the supply chain— be it the fulfillment company, the broker, or the transporters. In fact, NICB is aware of cases in which *all three* links were infiltrated through fraud, resulting in loads of cargo being released, brokered and transported by legitimate services but destined for criminal enterprises overseas.

These organized crime groups stay anonymous by remaining overseas, using legitimate brokers and transporters to move stolen goods to the groups' desired destinations for export. Many of these schemes involve business email compromises, carried out through phishing attacks or the use of slightly altered email domains.

NICB recently issued an alert detailing how criminals are exploiting cargo delivery systems and networks through Voice over Internet Protocol (VoIP) and synthetic identifications (IDs) to reroute electronics, medicine, clothing, food and beverages, and other goods.¹⁵

For example, VoIP has been exploited by criminals to spoof legitimate carrier contact information and area codes, all while remaining anonymous. They leverage these services to impersonate legitimate transporters, bid on shipments, and reroute freight to unauthorized drop locations. Unlike traditional cellular services, VoIP applications do not routinely create call detail records or provide cell site geolocational data—evidence typically utilized by law enforcement to aid in investigations—making it more difficult for law enforcement to identify criminal actors.

Similarly, criminals are using synthetic IDs and fraudulent documents to either acquire or re-route shipments to their preferred destinations. Instead of ending up on the shelf at your local store, goods are arriving on someone else's doorstep in another country.

As the shipping industry has grown more digitized and criminals more resourceful, cargo theft has become a crime of opportunity. But together, we have an opportunity to fight back.

V. Recommended Industry and Public Policy Responses

Regaining the upper hand against organized cargo theft demands both industry and public policy responses. From our unique vantage point and expertise, NICB offers the following recommendations.

a. <u>Industry Responses</u>

Detecting and preventing cargo theft requires a proactive, collaborative response across logistics, security, and law enforcement sectors. As cargo theft tactics grow more sophisticated, particularly with the rise of strategic and cyber-enabled schemes, industry professionals must commit to stronger carrier vetting, consistent driver identification checks, and the utilization of secure pickup protocols.

Ongoing education and training are also essential to improve awareness. Effective prevention depends on a balanced approach that combines consistent operational protocols and a stronger coordination between private industry and law enforcement agencies. Collaboration would also enhance intelligence within the industry, allowing for proactive analytics and enhanced identification of organized crime groups—and, ultimately, their prosecution.

¹⁵ "Digitalization of the Supply Chain Risks Exploitation and Increased Cargo Theft," National Insurance Crime Bureau (June 25, 2025) *available at* <u>https://www.nicb.org/news/news-releases/digitalization-supply-chain-risks-exploitation-and-increased-cargo-theft</u>.

Industry standards and certifications, such as those issued by the Transported Asset Protection Association (TAPA), are recognized as best practices in deterring and preventing cargo theft and thus should be incorporated into processes and procedures. Supply chain links should develop and conduct training on knowing how to respond, what information they should provide, and to whom they should report it in the event of a cargo crime.

Moreover, in addition to providing its members and law enforcement partners with support in identifying and investigating cargo crime, NICB's Cargo Program also conducts and participates in numerous training opportunities and conferences related to the protection of our nation's supply chains. These trainings aim to improve investigative outcomes, enhance interagency collaboration, and strengthen preventative measures to reduce the overall incidence of cargo theft. For any entity engaged in the supply chain, NICB recommends the following precautions:

Screen every employee. Conduct a background check on every employee including those with access to shipping information.

Train employees on the signs of cargo theft. Provide security training for every employee and educate drivers in hijack awareness and prevention as well as how to respond and report theft.

Check transportation partners before hiring. Partners should share your security philosophy, such as conducting background checks and employee training. Use freight brokers and transporters who do not permit practices that are prone to being exploited by criminals, such as double brokering. Ensure that only you as the shipper can make re-routing decisions and not the broker or transporter dispatch. Change orders should only originate from the owner of the cargo. Be cautious and always scrutinize emails to ensure that they are legitimate and not altered. Scrutinize and ensure phone numbers used by individuals within the supply chain are valid and, if determined to be VoIP, take additional vetting procedures.

Implement in-transit security measures. Cargo theft can be pre-planned or opportunistic and include an inside informant who follows the goods and ultimately leads criminals to quickly dispose of the cargo. Thieves will often wait outside known shipping facilities for drivers to stop. A best practice is to not stop within the first 200 miles, park in known secure locations and avoid "hot spots"—areas known for increased frequency of cargo crime.

Keep a vigilant eye. Trucks and cargo are most vulnerable when sitting idle. Use countersurveillance—observance and 360-visibility of your property and surroundings—in the duties of your security guards.

Take advantage of technology. Utilize layers of security: ensure that perimeters, entrances, building doors, and windows are well lit. Install alarm surveillance systems, vehicle and cargo tracking, immobilizers, and advanced security seals.

Conduct audits. Regularly look for gaps in shipment protection and stay abreast of how technology enables theft throughout the supply chain.

b. <u>Public Policy Responses</u>

Deterrence and coordination are key to fighting organized cargo theft. To date, however, the criminal networks that orchestrate these schemes have benefitted from a legal framework that does not provide adequate deterrence, as well as from a fragmented law enforcement and reporting environment.

Criminals should know that facilitating these crimes will put them behind bars. Additionally, victims along the supply chain—as well as law enforcement—should know precisely where to turn when thefts occur.

For these reasons, NICB strongly supports S. 1404, the Combating Organized Retail Crime Act (CORCA), which would strengthen federal criminal statutes to more effectively confront interstate and transnational organized theft.

S. 1404 would increase deterrence by providing for criminal forfeitures under Title 18 following convictions for the interstate shipment or transportation of stolen goods, as well as for the sale or receipt of stolen goods. Adding forfeiture as an additional tool for prosecutors sends a strong signal that it does not pay to facilitate or profit from cargo theft.

The bill also strengthens money laundering statutes, permits the aggregation of thefts in prosecutions, and would better enable the takedown of organized retail and supply chain criminal networks that use interstate or foreign commerce—such as the internet—to facilitate their crimes. Together, these are critical reforms needed to strengthen deterrence and confront a complex and highly organized threat landscape.

Additionally, S. 1404 would establish the Organized Retail and Supply Chain Crime Coordination Center within Homeland Security Investigations (HSI) at DHS. This vital reform will improve collaboration, data collection, and information-sharing between federal, state, and local law enforcement and would bring industry experts to the table to help ensure a coordinated approach to combating interstate and transnational organized crime. This center should be enabled to "connect the dots" by identifying trends and commonalities amongst cargo thefts to assist in exposing transnational organizations.

While industry has to date done its best to fill the gaps, there remains no uniform system or central repository for cargo crime reports or statistics, which has made understanding—and therefore effectively confronting—the full scope of the problem difficult. S. 1404 would address this by establishing a secure system for sharing information regarding organized theft, while

leveraging existing information systems at DHS and the Department of Justice, and tracking crime trends and releasing annual public reports on such trends.

Criminals are coordinated in their tactics, so law enforcement and industry must likewise be better coordinated in adopting countermeasures, as well as in encouraging and streamlining the reporting of these complex crimes to the appropriate agency for investigation. HSI is especially well-suited to operate this Coordination Center, given its longstanding expertise in combating transnational crime like cargo theft that threatens our economy and security here at home. NICB also supports the instruction that the Coordination Center establish relationships with state and local law enforcement, as well as with retail crime and cargo theft associations, and NICB stands ready to support the Center and provide any requested expertise, intelligence, and on-the-ground resources.

In addition to the much-needed reforms outlined in S. 1404, NICB would strongly support additional resources for dedicated investigative and prosecutorial units at DOJ that would focus exclusively on cargo theft as an increasing threat to our economy and national security.

NICB also notes that S. 1404, including its stronger tools for prosecutors and the contemplated Coordination Center at HSI, would serve as a force multiplier of other recent measures that protect consumers, including the INFORM Consumers Act, which Congress enacted in 2022, and S. 337, the Household Goods Shipping Consumer Protection Act, which was recently reported favorably by the Senate Commerce Committee. Together, these measures would be part of a vitally important fabric of deterrence and coordination that puts us all in the best position to combat these highly sophisticated supply chain crimes and the networks that facilitate them.

In short, NICB applauds the continued bipartisan work in the Senate to combat organized theft and criminal networks that harm Americans, and we urge the Committee to take up and favorably advance the Combating Organized Retail Crime Act to the floor.

c. <u>Public-Private Partnerships</u>

Finally, as NICB's history can attest, our collective fight against fraudsters and organized crime is strengthened through public-private partnerships. For decades, NICB has been a trusted partner of insurance commissioners and law enforcement across the country, assisting with investigations and facilitating vital information-sharing that helps uncover—and ultimately undo—complex insurance crime networks. We bring industry and government together in a shared mission of detecting, deterring, and preventing insurance crime.

In the same way, NICB stands ready to be a key source and facilitator for HSI within the cargo theft space, providing timely insights from our multi-carrier, multi-state vantage point into theft trends, tactics, recoveries, and all other valuable data points that would support the Coordination Center's mission.

VI. Conclusion

Chairman Grassley, Ranking Member Durbin, and Members of the Committee: thank you again for the opportunity to be here today. I look forward to answering any questions.