FOR SUBSCRIBERS

ARTIFICIAL INTELLIGENCE

Grand theft AI: Highway thieves are stealing millions in data center gear

Trucking, supply chain and security industry veterans detailed to NBC News how thieves staged dramatic robberies as part of the growing theft of tech equipment.

Listen to this article

00:00 14:31 1x



Valuable data center equipment is increasingly being targeted by organized criminal groups using deceptive techniques. Chelsea Stahl / NBC News; Getty

Oct. 26, 2026, 5:00 AM EDT

By Lisa Cavazuti

In early June, a trailer carrying some $13 million worth of computer server equipment headed east toward Fayetteville, Georgia, home to one of the largest data center developments in the country.

Following close behind was an unmarked sedan driven by two off-duty law enforcement officers hired to track the pricey technology to its final destination. Several hours into the trip, while on a stretch of interstate that cuts through the Mojave Desert, another car accelerated and struck the escort vehicle, forcing it to stop. Up ahead, the trailer sped away.

The trailer was found a day later at a truck yard in Stockton, California, not far from where the gear had originally been picked up. The pallets containing several hundred pounds of equipment were gone.

“The accident was not an accident. The bad guys wanted that load, so they intentionally took out the escorts,” said Gerardo Pachuca, who spent nearly two decades hunting down stolen cargo for the Los Angeles County Sheriff’s Department’s cargo criminal apprehension team before starting a private investigation firm.

About three weeks later, it happened again.

A trailer carrying server rack components estimated to be worth around $10 million was being escorted by a different company’s security team from San Jose, California, to a data center project in Texas. The cargo was also being monitored by an application tracking its location. Hours into the trip, the security team’s car was struck by an SUV in a hit-and-run-style collision that disabled the car. The trailer continued on, unchaperoned, tracking toward the planned destination.

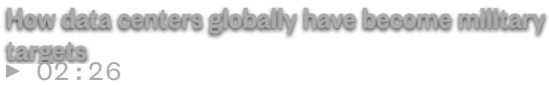
But the delivery was never made. The tracking coordinates had apparently been spoofed. Since then, neither shipment has been found.

The two thefts are the most extreme examples of a growing problem, investigators say. Since June, spurred on by the AI boom, thieves have made away with more than $100 million in data center freight, according to several industry leaders, consultants and investigators advising law enforcement in their investigation. Through records requests, interviews with law enforcement and executives in the freight industry, and review of industry “be on the lookout” incident bulletins, NBC News identified nearly two dozen cargo theft incidents of high-end technology in

states including California, Texas and Utah since last year. With tech giants plowing billions of dollars into new data centers, it's an issue that is only expected to grow.







Several cargo and security experts who formally advised the affected parties and law enforcement and informally helped through industry partners on the June investigations described the events to NBC News and provided industry bulletins detailing the incidents received by industry freight security councils.

Over the past two years, the value of the infrastructure used to build data centers has accelerated alongside the construction of projects across the country. Truckloads of costly equipment like servers, fiber-optic cables, computer memory chips, copper wires and bitcoin mining machines crisscrossing America's highways have become prime targets for organized criminal groups looking for big payoffs, according to law enforcement and industry experts. The components used to construct data centers have seen a dramatic increase in price in line with demand,

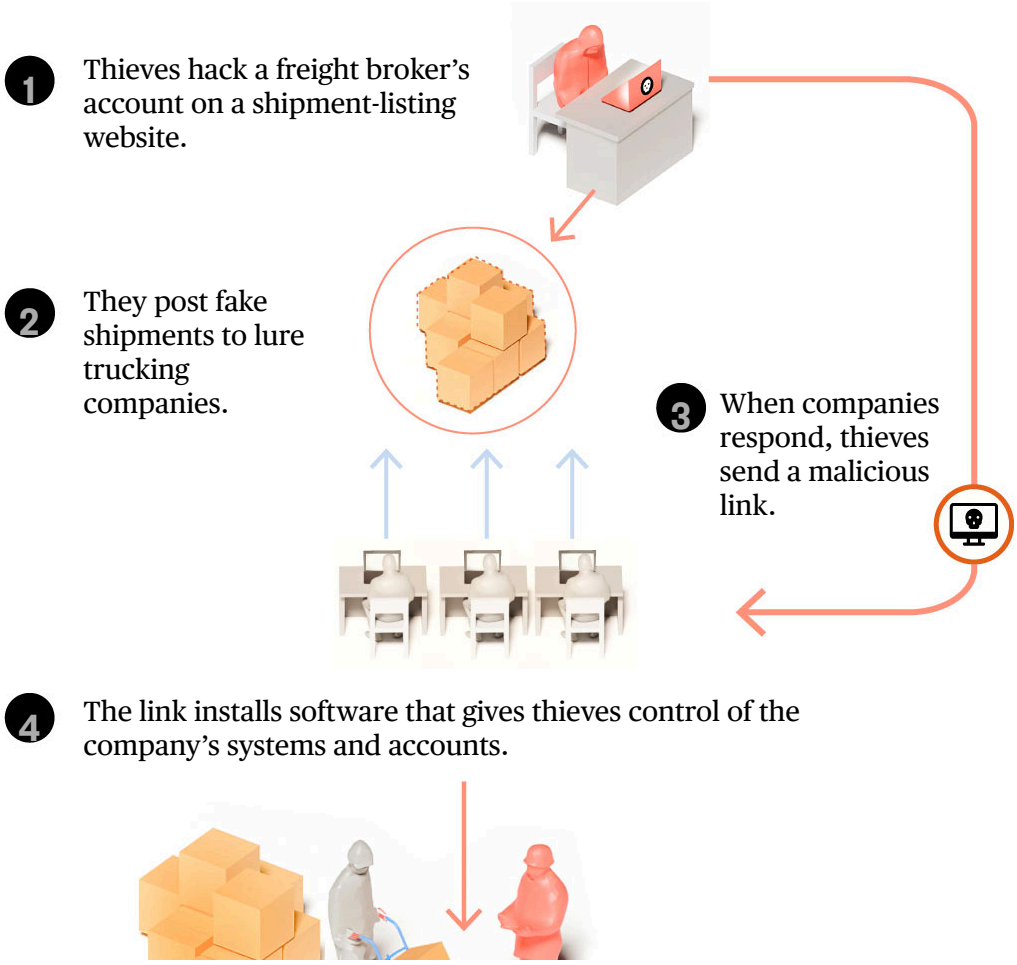
creating more frequent opportunities for criminals who can resell the big-ticket equipment abroad or break them down for parts.

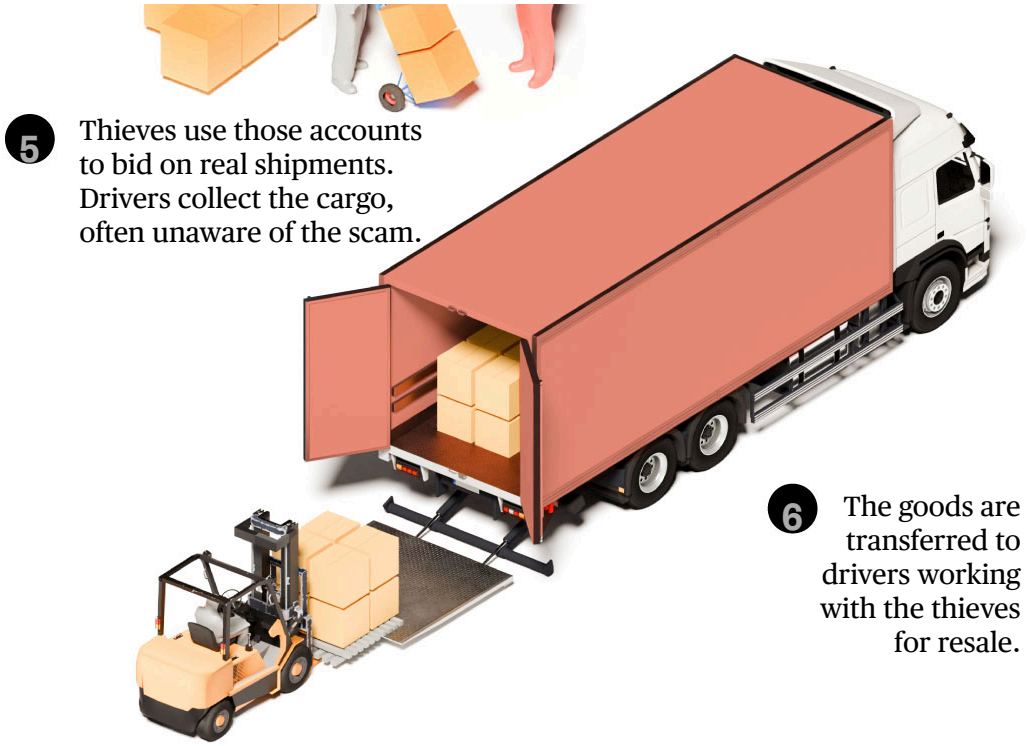
The AI boom brought with it increased opportunity to steal highly sought equipment and coincided with a post-Covid shift by thieves from more traditional hijacking tactics to globally connected criminal networks using fraudulent schemes to steal goods. Thieves' digital strategies – like compromising freight brokers' and carriers' accounts in order to gain access to proprietary shipping schedules or stealing the identities of legitimate trucking companies to secure high-value shipments – have upended supply chain security, helping groups target valuable shipments more precisely.

That transition came about as the pandemic forced verification and onboarding workflows for freight carriers, once highly reliant on personal relationships, online. Using cyber-enabled tactics, criminals are more easily able to skirt security protocols using VPNs and other spoofing technology to deflect law enforcement and tracking systems.

How a method of strategic cargo theft works

By taking over a freight company's online accounts, thieves can arrange real pickups and redirect the goods for resale.





Source: FBI

Graphic: Javier Zarracina / NBC News

"It's like stealing pure gold bars," said Keith Lewis, head of operations at risk-assessment firm Verisk CargoNet, whose team tracks cargo theft incidents and has seen elements tied to AI infrastructure – like copper wires, enterprise servers, RAM modules, storage drives and fiber-optic components – increasingly targeted by theft groups this year. "We've seen some of these thefts go up into 30-plus million dollars for one particular shipment. It's so much easier to steal this than to rob a bank."

The examples are piling up.

In July, an estimated $38 million of cables and cartridges were stolen in Reno, Nevada, by drivers using fake licenses and scheduled to be flown overseas to Asia, according to individuals assisting with the investigation.



A still image of stolen copper wire recovered at a truck yard in Cook County, Illinois in June.

Cook County Sheriff's Office

In June, Michael Kruzel, an investigator with the Cook County Sheriff's Office in Illinois, got a tip that a trailer full of merchandise stolen in Pine Hill, Alabama, had been detected at a truck yard in northern Illinois. That initial trailer led him to a second one parked nearby, discovering in total $1.3 million worth of copper wire spools and custom-made data center modular power solutions equipment bound for an infrastructure project in Texas.

In April, the Los Angeles County Sheriff's Department recovered several boxes of data center cooling equipment at a warehouse alongside other stolen items, including nicotine pouches, televisions, apparel and speakers.

Some pastors have embraced data centers; others worry about harm to their communities

02:57



Last year, tens of millions of dollars of enterprise hardware equipment, including server racks, routers and memory modules, intended for an AI data center were stolen in separate incidents after leaving shipping facilities in Salt Lake City. One shipment was later tracked to Irwindale, California, near the Port of Long Beach, and the Los Angeles County Sheriff's Department made an arrest.

"Things that are precursors for the AI data centers: copper, server racks and RAM. Those are the things that are the precursors to build one, so that's what we're seeing the big increase in," said Lewis, who works with law enforcement to deter thefts and recover stolen goods. "It's the dollar value that's getting the attention because the product they're stealing costs so much more."

Cargo experts say AI-related equipment does not commonly end up on online marketplaces, unlike consumer goods. In some instances, before technological equipment is stolen, thieves have already identified buyers, many of whom are overseas where component parts may be less readily available or gray-market parts can be used to bring project costs down. It is widely understood by law enforcement officials that stolen equipment winds up in countries, including China, that are affected by the U.S.' strict export controls of AI equipment.

"It's a global playing field now," said Lewis, whose team assisted in recovering bitcoin mining machines that were stolen last year in Los Angeles and found at Dallas Fort Worth Airport loaded onto a plane bound for Asia the following day.

That reality has coincided with the rise of what some experts call “strategic” cargo theft tactics, which involve thieves using deceptive techniques, including email infiltration and shipment misdirection, to identify specific valuable loads to pursue ahead of time, instead of stealing opportunistically, as was common in the past.

Additionally, there are inconsistencies in the investment in security measures taken by manufacturers and carriers to track the goods being transported.

Verisk CargoNet’s most recent analysis found that incident counts of theft of all cargo declined 26% in the second quarter of 2026 from the same time last year, but the severity of thefts rose, driven by a concentration of several extreme multimillion-dollar losses of technological freight targeted. The total estimated cargo losses more than doubled year over year, reaching $304.6 million in the second quarter of 2026, up from $135.7 million a year earlier, with food and beverage and metals being the top stolen commodities, according to the analysis.

At the federal level, the FBI elevated the issue in April by issuing a warning that “cyber-enabled strategic cargo theft” is surging nationwide. Cyber tactics – such as hacking into carriers’ emails to identify specific valuable loads to steal, “load boards” where transit jobs are posted and bid for, disrupting GPS tracking applications, or using AI to generate fake driver’s licenses – now play a major role in criminals’ abilities to carry out thefts, according to law enforcement investigators and consultants.

“That’s how most of it is being done,” said Sgt. David Pantoja of the Los Angeles County Sheriff’s Department, who leads the cargo criminal apprehension team.

In total, the National Insurance Crime Bureau estimates that theft of all cargo now costs the U.S. economy $35 billion annually. Estimated cargo theft losses rose to nearly $725 million in 2025, up 60% from 2024. The American Trucking Associations says cargo theft has increased 1,500% since 2021.

“Right now the surge is at its max that I’ve seen it,” Pachuca said.

While the two hit-and-run-style thefts in June remain isolated incidents in the tactical strategies used, freight experts view them as first of their kind, intentional and representative of an escalation of violent tactics used in the United States akin to methods typically seen elsewhere, such as in Mexico, Brazil and Europe.

“These are extremely high-level organized rings that are operating from a dozen different countries, targeting freight in the United States supply chain. These are not unsophisticated crews just pulling off theft,” said Scott Cornell, chair of the Transported Asset Protection

Association, Americas, or TAPA Americas, the largest global nonprofit organization dedicated to supply chain security standards and education, who has spent more than 30 years investigating cargo theft cases, partnering with law enforcement task forces. “They’re planned. They’re plotted. They’re strategic. They’re playing chess in the supply chain.”

Yet, it’s the breakdown of vetting processes, not the traffic collisions themselves, that stands out to experts like Cornell. “The only way this works is if the drivers are not properly vetted,” Cornell said, who is also a Crime & Theft Specialist at SPG Cargo & Logistics.

So far this year, India, Uzbekistan, Pakistan, Colombia and Moldova are among the regions with the highest rates of suspicious or fraudulent activity associated with cargo theft in the U.S., according to Verified Carrier, a digital platform used by freight carriers, brokers and shippers to vet and verify driver and carrier identities.

“So you have the head of the snake overseas, which makes it very difficult for not only the industry, but law enforcement here in the United States,” Cornell said. “They’re making great arrests, but the people they’re arresting are not the head of the snake.”

Investigators say the problem extends far beyond the individuals carrying out the thefts on U.S. soil.

“Cargo thefts are not the result of small operations. These are well-funded, sophisticated criminal businesses, which include Mexican drug cartels as well as operations out of West Africa, China and Eastern Europe,” David Glawe, president and CEO of the National Insurance Crime Bureau, shared in testimony before the Senate last year.

In the past two years, more logistics companies have requested security services, according to Mike Duffy, co-founder and CEO of Solutions Group International, a security escort company based in Southern California, where much of the high-value goods are being manufactured.

“We’re escorting hundreds of loads per month,” Duffy said, much of it associated with data centers, in interstate trips across the country from distribution centers through the point of delivery, documenting every stop. Threshold levels that usually require a security escort begin around $800,000, according to Duffy, but as values for AI technology have risen, manufacturers and insurance companies typically recommend or mandate the use of security escorts.

The phenomenon has prompted bipartisan action in Washington. Congress is weighing the Combating Organized Retail Crime Act, legislation designed to strengthen federal response by creating a coordination center within Homeland Security Investigations, improving intelligence

sharing and expanding prosecutors' ability to pursue interstate theft networks. The bill is under consideration by the Senate Judiciary Committee after being approved by the House in May.

States such as Arizona, California, Tennessee and Illinois have established or expanded specialized cargo theft task forces that bring together state and local police, prosecutors, and industry partners to investigate theft rings operating across jurisdictions.

Donna Lemm is the chief strategy officer at IMC Logistics, a major logistics company based in Memphis, Tennessee. In May 2024, Lemm said, IMC was targeted by seven cars storming the company's gates in the middle of the night – the first time thefts had occurred at any of the company's 54 terminals across the country. That incident – what Lemm calls her "aha moment" – led her to testify before the Senate last year and advocate for federal intervention.

"While we do see strategic thefts targeting valuable goods, we can't lose sight of all the goods that are being stolen across the spectrum," Lemm said, citing agricultural and consumer goods as examples of cargo most commonly stolen. "The impact is huge to the American consumer, who has no idea how this rolls down to them. People are stealing from us, and we got to stop it."

Lisa Cavazuti

Lisa Cavazuti is a producer and reporter for the NBC News Investigative Unit.
