Cooley

White House Targets Trade Fraud With AI

September 3, 2026

The White House recently announced that “the age of untraceable illegal transshipment is over.” In an August 13 report titled, “The Great Transshipment Scam,” the White House Office of Trade and Manufacturing Policy issued what it called a “warning to the world” – “stop evading and avoiding the Trump tariffs through illegal transshipment. Those who continue will be caught.”

Illegal transshipment, which is the practice of routing goods from higher-tariff countries through lower-tariff jurisdictions to evade US tariffs, reportedly costs America tens of billions of dollars annually. To counter illegal transshipment, US Customs and Border Protection (CBP) is developing an AI-enabled “detective border” that will analyze shipment data, routing histories, product classifications and other information to purportedly “reveal[] inconsistencies that no human could catch at scale.”

On the same day the White House report was released, the US Department of Justice (DOJ) issued a memorandum identifying trade fraud as a top enforcement priority, underscoring the risk of criminal prosecution for companies and individuals engaged in tariff evasion or other fraud schemes.

The government’s focus on illegal transshipment can affect any company engaged in foreign commerce, but those connected to China supply chains should pay particular attention. Now is a good time to evaluate import practices, strengthen compliance programs and prepare for this new era of data-driven enforcement.

CBP’s new AI ‘detective border’

The White House report estimates that transshipment “is draining the US treasury” of $10 billion to $100+ billion in lost tariff revenue each year.

According to the report, since the first Trump administration imposed Section 301 tariffs on China in 2018, goods that previously moved directly from China to the US are increasingly being routed through third-country jurisdictions – including Vietnam, Malaysia, Thailand, Mexico and Cambodia – to take advantage of lower tariff rates. The report makes clear that the government is aware of these routing patterns and views them as a principal driver of tariff revenue losses. Other higher-tariff countries are allegedly beginning to adopt similar practices, but China-origin transshipment remains the enforcement priority.

One step being taken to counter transshipment is the development of an AI-enabled “detective border.” The AI detective border is described as an “AI-driven net that never sleeps, never tires, and never forgets.” The AI architecture will fuse “anomaly detection, link analysis, capacity validation, and mirrored-flow verification into a single predictive platform.” The platform will continuously analyze data to attempt to identify “anomalous routing patterns, suspicious bills of lading, false-origin claims, value mismatches, and capacity inconsistencies.” Additionally, AI will play a role in identifying potential mismatches between a product’s “digital identity” and its “physical reality” by analyzing “container markings, packaging patterns, and X-ray imaging.” CBP will leverage these findings to bring enforcement actions.

DOJ memo outlines enforcement priorities for fraud

Also on August 13, the National Fraud Enforcement Division (NFED) issued a memorandum setting forth its enforcement priorities. As we discussed previously, the NFED is a new division within the DOJ for investigating and prosecuting fraud against federal government programs.

The memo states that the NFED will utilize sophisticated data analytics tools and other new technology to build a “data-driven white-collar law enforcement” group. The NFED is expected to have 500 attorneys and other staff by late August and will “continue to rapidly grow for the next two years.”

The memo identifies five enforcement priorities:

1. **Global trade and commerce**, which will target “illicit transshipment schemes, country-of-origin fraud, the

undervaluation of imported goods designed to evade duties, sanctions evasion, and foreign forced labor schemes."

2. **Public trust and financial integrity**, including government procurement fraud (such as bid rigging, self-dealing and billing fraud), as well as benefit and grant programs (such as student loans and small business programs).
3. **Healthcare**, such as Medicare or Medicaid fraud, controlled substance diversion, home health and hospice schemes, and deceptive marketing of unsafe products and services.
4. **Internal revenue**, which will focus on criminal tax enforcement.
5. **Corporate misconduct**, which will focus on "fraud and other economic crimes."

Echoing the White House report, the memo emphasizes that trade fraud and customs evasion "undermine American industry" and "deprive the public fisc of vital external revenue."

Implications

With the administration viewing trade fraud as a significant threat to American industry and the broader US economy, companies with global supply chains should expect heightened scrutiny of their import practices. That scrutiny will be increasingly data-driven and take advantage of new technology. The consequences of noncompliance may extend beyond civil penalties to criminal prosecution. Companies should consider reviewing and strengthening their compliance programs to identify and address potential issues or weaknesses in their supply chain.

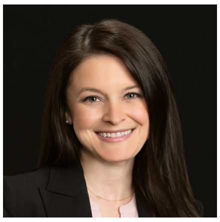
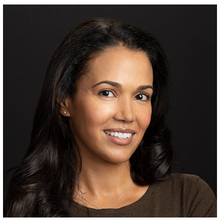
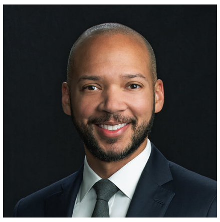
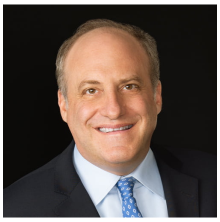
Companies that receive notice that they are the subject of a trade fraud investigation – whether through a CBP Request for Information, a subpoena or Civil Investigative Demand from the DOJ, or a formal notice of detention or seizure – should act quickly and deliberately to evaluate the allegations and potential defenses. Companies with China-connected supply chains should be particularly alert, as enforcement agencies are actively scrutinizing import patterns involving Chinese-origin goods routed through third countries.

As an initial matter, companies should retain experienced counsel before responding to any government inquiry or making statements to investigators. Companies should also take immediate steps to preserve all potentially relevant documents and data, including shipping records, customs filings, supplier agreements and internal communications relating to import practices. In parallel, companies should consider initiating an internal investigation to assess the scope of the issue, determine whether voluntary self-disclosure is appropriate and develop a strategy for engaging with the government. Throughout this process, companies should be mindful that trade fraud investigations often involve multiple agencies – including CBP, DOJ and the Department of Commerce – and that early coordination across enforcement tracks is critical.

How we can help

Cooley's global Tariffs Task Force is a team of high-stakes litigators, former prosecutors, including the former chief of the public corruption unit of the US Attorney's office, and investigation counsel. We have extensive experience in cross-border investigations, particularly those involving Asia and China, and our team includes Mandarin-speaking lawyers who can communicate directly with clients and counterparties in their native language. Companies that receive an inquiry or notice that indicates they may be the subject of a government investigation can reach a member of our team by emailing zCooleyTariffsTeam@cooley.com.

Contributors

			
Amanda Main	**Shamis Beckley**	**John Bostic**	**Andrew Goldstein**
Bio	Bio	Bio	Bio

Will Pao
Bio