HEALTHCARE

September 2026

Preparing Your Company's Data for Trade Compliance Investigations

PREPARED BY: JOSHUA GALUSKA, HEATHER BATES, AND MASON PAN

INTELLIGENCE THAT WORKS

The Enforcement Landscape

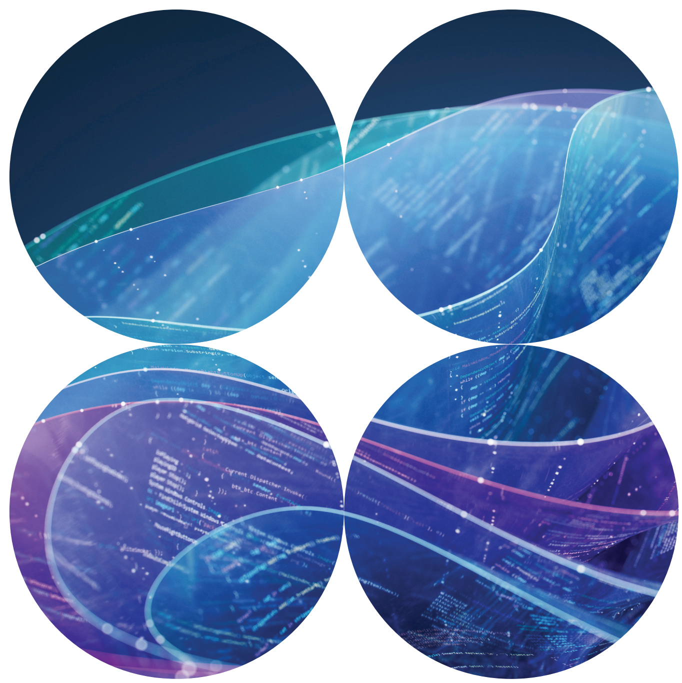
In August 2025, the United States Department of Justice (DOJ) and Department of Homeland Security (DHS) launched the Trade Fraud Task Force (TFTF) to investigate and prosecute misrepresentations to US Customs and Border Protection (CBP). In its first year, the TFTF surpassed $1 billion in civil and criminal recoveries, penalties, forfeitures, and alleged losses in pending cases. The majority of this has come from civil enforcement under the federal False Claims Act (FCA), which highlights the government's increasing use of the FCA to enforce trade compliance.

The DOJ's prioritization of customs compliance shows no signs of abating. Earlier this year, Deputy Assistant Attorney General Brenna Jenny reported an increase of more than 50 percent in new FCA whistleblower complaints alleging duty evasion compared to prior years and the highest number of FCA customs and trade fraud settlements in a single year.[1] She also highlighted three common categories of duty evasion misconduct: misclassification, undervaluation, and misstatement of country of origin.

Beyond duty evasion, FCA liability is a risk for companies that sell products to the US government in violation of trade compliance commitments. Federal contractors may be required to certify that products offered to government customers (e.g., US Department of Veterans Affairs) are manufactured in designated countries or meet domestic-content requirements under the Trade Agreements Act (TAA) or Buy American Act (BAA). A company that knowingly sells noncompliant products but certifies compliance with those requirements may create FCA exposure even if the products were declared correctly at customs.

These priorities share a common feature: each leaves a data trail. Trade compliance allegations can be reconstructed through data and tested analytically using customs declarations, company sales records, supplier documentation, and logistics data. DOJ is already using data analytics to drive its enforcement. In February 2026, TFTF Head Cody Matthew Herche noted that the task force uses comprehensive customs datasets like the Automated Commercial Environment (ACE) and advanced analytics, including reexamination of historical data, to identify anomalies and generate investigative leads.[2]

The government expects companies to maintain data and documentation supporting their customs declarations, and federal contractors may need data supporting applicable country-of-origin representations.[3] Companies that have already mapped their data landscape can better produce a coherent, data-driven compliance narrative in response to a government investigation.



1 Remarks by Brenna Jenny, Deputy Assistant Attorney General, Commercial Litigation Branch, DOJ Civil Division, "FCA Enforcement Priorities," keynote luncheon, Federal Bar Association 2026 Annual Qui Tam Conference, Washington, DC (February 19, 2026).

2 Remarks by Cody Matthew Herche, Senior Counsel, DOJ Criminal Division, and Head of Trade Fraud Task Force, keynote address, ACI International Trade Investigations, Enforcement & Litigation Conference, Arlington, Virginia (February 23, 2026).

3 For example, under Section 484 of the Tariff Act, the importer of record is responsible for using reasonable care to enter, classify, and determine the value of imported merchandise and provide any other information necessary to enable the CBP to properly assess duties, collect accurate statistics, and determine whether other applicable legal requirements, if any, have been met.

The Fragmentation Problem

Most companies operate in data silos. Sales and shipment data are stored in enterprise resource planning (ERP) systems. Customs declarations often reside with brokers. Supplier and procurement data live in separate logistics databases. Key logistical data may also be held by third parties along the company's supply chain. Government contracts and procurement records, including applicable TAA/BAA representations and certifications, typically sit in yet another system. Each system may function well within its own domain but is rarely designed to facilitate the end-to-end tracing required to demonstrate compliance with TAA/BAA requirements for applicable products sold to the government or compliance with import restrictions, customs requirements, and duty obligations.

When an enforcement action arrives, companies must reconstruct a coherent picture across their disparate data systems simultaneously. Data fragmentation creates three challenges. First, gaps emerge where transactions fall out between systems and the end product represented as compliant with country-of-origin requirements that cannot be traced back to where the product was manufactured. Second, inconsistencies arise where the same product carries different origin, classification, or valuation in different databases. Third, latency becomes a critical constraint: the time required to manually reconcile disconnected datasets under enforcement timelines can delay the company's ability to respond to and address investigators' concerns. In each case, a data architecture limitation can be perceived as a compliance failure or an intentional misrepresentation.

Data Assessment Companies Should Do Today

Based on BRG's experience assisting clients in response to government investigations and customs enforcement matters, we recommend that companies with material trade compliance exposure take practical steps to ensure their data systems are prepared for the key questions regulators ask.

1. **Inventory data systems.** Identify every system that holds trade-relevant data. Document what data each system holds, how long records are retained, what archive processes are in place, and how archived data can be retrieved and extracted in a format suitable for analysis.
2. **Map system owners.** For each system, identify the technical owner who can grant access and extract data; and the business owner who can explain how the data is created, what the data represents, and how the business uses it. Given personnel turnover, maintain a current system ownership inventory that is updated as employee responsibilities change.
3. **Document business processes end to end.** Trace how a product moves from raw material sourcing through manufacturing, intermediary transactions, border entry, and final sale. Map each step in the supply chain to the system where the data is recorded.
4. **Identify the data you do not own.** Inventory vendors and other third parties in the supply chain and border-entry processes, as well as the data they hold with respect to your raw materials and finished goods. Develop contractually defined processes to access live and archived data from third parties necessary to construct your end-to-end supply chain narrative.
5. **Test data connectivity.** Determine whether systems can be linked through common identifiers (e.g., serial number). If not, understand the magnitude of the manual effort required to connect the. Evaluate the costs and benefits of designing a technical process to facilitate linking systems ahead of any government inquiries.
6. **Conduct a simulated data request.** Identify the questions a regulator would likely ask, and attempt to answer them using existing data. For example:
   a. Can this sale to a government customer, such as the US Department of Veterans Affairs, be traced back to procurement and manufacturing data sufficient to support our country-of-origin representation?
   b. What is our process for assigning Harmonized Tariff Schedule codes to our imported products. How is accuracy validated on a regular basis?

Conclusion

Data analytics has become central to trade compliance enforcement as a tool the government uses to identify investigative leads and the foundation on which companies must build their defense. The companies that navigate this landscape effectively will prepare their data today to answer tomorrow's questions. Those that understand their systems, business processes, and data connectivity gaps will best position themselves to assert compliance with policy and prove compliance through data.

KEY PROFESSIONALS

Heather Bates
Managing Director
hbates@thinkbrg.com

Joshua Galuska
Director
jgaluska@thinkbrg.com

Mason Pan
Managing Director
mpan@thinkbrg.com

BRG combines world-leading academic credentials with world-tested business expertise, purpose-built for agility and connectivity, which sets us apart—and gets you ahead.

Our top-tier professionals include specialist consultants, industry experts, renowned academics, and leading-edge data scientists. Together, they bring a diversity of proven real-world experience to economics, disputes, and investigations; corporate finance; and performance improvement services that address the most complex challenges for organizations across the globe.

Our unique structure nurtures the interdisciplinary relationships that give us the edge, laying the groundwork for more informed insights and more original, incisive thinking from diverse perspectives that, when paired with our global reach and resources, make us uniquely capable to address our clients' challenges.

VISIT THINKBRG.COM TO LEARN MORE.