January 20, 2026

Mr. Joseph Martella
Cargo and Conveyance Security
Office of Field Operations
U.S. Customs & Border Protection
1300 Pennsylvania Ave NW
Washington, DC 20004

RE: Enhanced Air Cargo Advance Screening (ACAS) – USCBP-2025-0053

On behalf of the National Retail Federation, we are providing comments regarding U.S. Customs and Border Protection's Interim Final Rule on Enhanced Air Cargo Advance Screening (ACAS). While NRF and its members greatly appreciate and support CBP's cargo security mission, our members have raised a few issues and concerns with the ACAS IFR. We believe that addressing the issues below will help ensure a smooth transition and implementation of the updates to ACAS in the IFR.

NRF passionately advocates for the people, brands, policies and ideas that help retail succeed. Retail is the nation's largest private-sector employer, contributing $5.3 trillion to annual GDP and supporting one in four U.S. jobs — 55 million working Americans. NRF empowers the industry that powers the economy. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities.

Clarification and Notice and Comment for New Data Requirements

CBP should clarify that enforcement of the new ACAS data transmission requirements will not be enforced during the 12-month implementation period. This is critical for entities that are engaging in the process in a good faith manner to adjust to the new rules. It is unclear whether CBP will utilize informed compliance or enforcement restraint only for carriers making "significant progress" and "good faith effort" toward compliance. The terms remain undefined and subjective. The rule explicitly states "willful and egregious violators will be subject to enforcement actions at all times" without clearly defining what constitutes such behavior, creating immediate penalty exposure up to $100,000 per conveyance arrival even during the allowed grace period.

Such enforcement discretion is critical for industry and customers to successfully implement these new obligations. CBP has certainly used such enforcement discretion when implementing significant new programs such as ACAS and even the Importer Security Filing. The new data elements requirement for ACAS represents a significant expansion requiring substantial compliance efforts across the entire air cargo supply chain — including air carriers, customs

brokers, ACAS filers, shippers and ecommerce marketplaces. Clarity on the implementation period absent fear of punishment for good faith actors, coupled with robust consultation with the trade community, will be necessary for long-term success of these changes.

In addition, CBP should ensure that entities sharing data received from third parties are not held liable for inaccuracies that they cannot verify. There are new data elements that industry can seek from customers, but verification of that information would be logistically and extremely difficult (such as newly required consignee information). Parties submitting data should not be responsible for conducting due diligence beyond what is already currently required.

Particularly Burdensome Data Elements: Unmasked IP/MAC Addresses and Other Privacy-Sensitive Requirements

We would request that CBP not require the data element of Unmasked IP/MAC Addresses. This new data element requirement likely creates irreconcilable conflicts with data protection regulations in multiple jurisdictions. These technical identifiers are considered personally identifiable information (PII) under many privacy regimes and protected as such. Requiring this information would force companies to choose between CBP compliance and local law adherence. In addition, biographic data collection from government-issued photo identification represents excessive personal data collection for routine shipping activities, creating high-value targets for data breaches and identity theft exposure.

In addition, collection of unmasked IP/MAC addresses is technically infeasible for many business models, particularly transactions where shippers lack access to consignee device information. It is unclear how stakeholders could sufficiently adhere to this requirement.

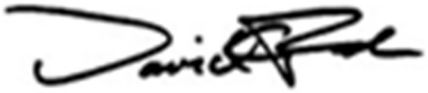
Clarification of Verified Known Consignor Program

CBP should provide comprehensive clarification of the Verified Known Consignor program, including application procedures, eligibility criteria, approval timelines and recognition of existing security certifications. CBP should maintain the new data requirements as optional until at least 12 months after such clarification is published. CBP should also ensure that multiple types of parties are able to qualify as VKCs or VKC equivalent programs and ensure that good faith actors that are able to transmit to CBP the information on the shipper, where a product comes from, and where a product ships to, can qualify as VKC-compliant.

In addition, VKC designation is the critical factor determining applicability of conditional requirements, yet the current lack of program details creates an impossible situation: companies must simultaneously pursue VKC designation while building systems to collect conditional data elements, without knowing which compliance path will prove viable. The arbitrary authority of CBP to recognize or revoke VKC status discourages investment in compliance programs since companies cannot confidently plan strategies when recognition can be unilaterally withdrawn based on undisclosed standards. Until the VKC program is fully defined and accessible, the conditional requirements that depend on VKC status should remain optional.

NRF appreciates the opportunity to provide comments on this matter. If you have any questions, please contact me or Jonathan Gold, NRF's vice president of supply chain and customs policy.

Sincerely,



David French
Executive Vice President
Government Relations