White Paper

Why Retailers and Importers Must Invest in AI-Enabled Product Safety & e-Filing Compliance Infrastructure

Executive Summary

Global sourcing has transformed how consumer products reach U.S. markets. Retailers and importers increasingly rely on complex, cross-border manufacturing networks to maintain competitive pricing, product diversity, and speed to market. At the same time, the regulatory environment governing consumer product safety is becoming more data-driven, enforcement-oriented, and operationally demanding.

The enacted amendments to 16 CFR 1110[1], establishing what is known as the U.S. Consumer Product Safety Commission's e-Filing Rule, mark a structural shift in how imported product compliance is evaluated. The new e-Filing Rule does not merely change import filing requirements—it represents a fundamental shift toward continuous, data-driven verification of product safety and certification integrity at scale, tied directly to product identity and supply chain traceability.

Traditional approaches to imported product compliance—spreadsheet tracking, static document repositories, periodic audits, and manual verification upon request—were not designed for real-time regulatory data exchange across high-volume import operations. As enforcement expectations evolve, retailers and importers must adopt integrated compliance infrastructure capable of continuous documentation management, automated validation, and audit-ready evidence retention.

This paper explores the increasing risks faced by retailers and importers and outlines a modern compliance architecture tailored to these environments: an AI-enabled, end-to-end framework that integrates testing data management, supplier verification, regulatory mapping, lifecycle monitoring, and documentation governance. Properly implemented, this infrastructure transforms compliance from an episodic obligation into an operational capability that reduces product incident and enforcement exposure, supports import continuity, and strengthens organizational resilience.

Global Sourcing Growth and Structural Compliance Risk

Retailers and importers today operate within distributed manufacturing ecosystems spanning multiple jurisdictions, suppliers, and production cycles. While this model delivers commercial flexibility, it introduces systemic compliance risks that scale with product volume and supply chain complexity.

[1] See, e.g., eFiling – CPSC's Modern Approach for Filing Certificate Data, CPSC's e-Filing Website; found at https://www.cpsc.gov/eFiling.

Common exposure areas include:

- Incomplete or outdated product testing documentation
- Certification traceability gaps
- Supplier documentation inconsistencies
- Labeling or standards misalignment
- Cross-jurisdiction regulatory variability
- Import recordkeeping deficiencies
- Data integrity failures

Unlike legacy import and retail regimes where verification may have been limited to post-entry document review, modern regulatory expectations increasingly require real-time access to structured compliance data. Failures can trigger shipment holds, corrective actions, recalls, enforcement scrutiny, and reputational harm.

Importers—not foreign manufacturers—bear primary responsibility for ensuring that regulated products entering U.S. commerce meet safety requirements and that compliance documentation is accurate, accessible, and verifiable.

Regulatory Shift: e-Filing as Operational Compliance Infrastructure

The CPSC's e-Filing requirements represent more than a modernization of customs reporting. It signals a move toward continuous regulator visibility into importer compliance systems and performance.

At a high level, the rule requires importers to electronically transmit standardized product safety data tied to:

- Applicable safety rules
- Certification status
- Testing documentation
- Product identifiers
- Supply chain traceability

The practical implication is that compliance data must be structured, current, and consistently linked to specific products—not scattered across disconnected repositories.

For compliance professionals, e-Filing introduces operational questions:

- How is testing data validated and version-controlled?

- Can documentation be matched reliably to specific SKUs or product batches?
- Are supplier certifications continuously monitored?
- Is compliance data audit-ready at any moment?

Manual systems introduce latency, human error, and fragmentation—conditions incompatible with a high-volume electronic regulatory exchange.

Aggressive Enforcement Environment

The CPSC has both articulated and demonstrated an increasing emphasis on proactive safety verification and early intervention, particularly with respect to imported goods.[2] In 2025, the agency issued a record 422 product safety recalls—a 38% increase over the prior year.[3] When combined with unilateral warnings issued, that total rises to 542 actions—averaging more than ten per week.[4] Notably, while recall frequency increased significantly, the number of units recalled declined by nearly 50% year-over-year, and reported incidents associated with those products fell by 28% compared to 2024 and 56% compared to 2023.[5] This divergence strongly suggests that the Commission is intervening earlier in the product lifecycle, acting before noncompliant or potentially hazardous products achieve broad market penetration.

There is also a meaningful shift in the regulatory basis for these actions. In 2025, nearly half of all recalls cited regulatory violations rather than product defects—approximately double the proportion observed in 2022.[6] This trend reflects a broadened enforcement focus: not only on products containing a defect that could create a substantial product hazard, but also on products that fail to satisfy applicable statutory or regulatory requirements regardless of whether a potential hazard has been identified.[7] For importers and retailers, this underscores a critical reality—regulatory compliance itself has become an independent enforcement priority. Verification of conformity with applicable safety rules must occur prior to importation and sale, not after an issue arises.

The geographic concentration of recalls further reinforces this posture. In 2025, 71% of recalled products were manufactured in China, consistent with the Commission's heightened scrutiny of imported consumer goods.[8] The implementation of electronic importer submissions significantly increases regulator visibility into compliance and practices for foreign-manufactured products. Enhanced data transparency allows regulators to identify noncompliance, incomplete

---

[2] See, e.g., Acting Chairman Feldman Highlights Key Safety Accomplishments of President Trump's CPSC, Statement of Acting Chairman Peter A. Feldman (Jan. 20, 2026); found at: https://www.cpsc.gov/About-CPSC/Chairman/Peter-A-Feldman/Statement/Acting-Chairman-Feldman-Highlights-Key-Safety-Accomplishments-of-President-Trumps-CPSC.

[3] An Analysis of Consumer Product Recalls in 2025, Don Mays, Product Safety Insights LLC (Feb. 2026); found at: https://lnkd.in/e9YtSHzQ.

[4] *Id*.

[5] *Id*.

[6] *Id*.

[7] For the 208 recalls for regulatory violations in 2025, only two minor injuries were noted in total. *See id*.

[8] *Id*.

documentation, and systemic control weaknesses more efficiently and at greater scale. Import compliance risk is therefore shifting from episodic, shipment-level inspection to broader programmatic evaluation.

In this environment, importers and retailers that cannot demonstrate disciplined compliance governance may face:

- Shipment delays or holds
- Mandatory corrective action plans
- Escalated enforcement scrutiny
- Expanded audits or information demands
- Reputational and commercial consequences

Compliance readiness now depends on infrastructure capable of preserving data integrity, maintaining defensible audit trails, and ensuring continuity of testing, certification, and documentation controls across the product lifecycle. Consequences for violations can be severe. Just this past year, the Commission, working with the U.S. Department of Justice ("DOJ"), secured criminal sentences against executives of the domestic subsidiary of a China-based electronics firm for violating the Consumer Product Safety Act.[9] They also obtained a guilty plea to other criminal charges in a separate matter.[10] And in the civil arena, the CPSC imposed $38.4 million in penalties and restitution against companies the agency determined was violating U.S. product safety laws.[11]

Prosecutorial Standards and Modern Compliance Expectations

The U.S. Department of Justice ("DOJ") evaluates corporate compliance programs through a structured and demanding framework.[12] Prosecutors are directed to examine three core questions: Is the program well designed? Is it applied earnestly and in good faith—meaning adequately resourced and empowered? And does it work in practice? These inquiries extend beyond written policies to assess whether compliance systems are operationally embedded, risk-informed, data-enabled, and capable of detecting and addressing violations before they result in regulatory intervention.

---

[9] Two Corporate Executives Sentenced in First-Ever Criminal Prosecution for Failure to Report Under Consumer Product Safety Act, Dept of Justice Press Release (June 16, 2025); found at: https://www.justice.gov/opa/pr/two-corporate-executives-sentenced-first-ever-criminal-prosecution-failure-report-under.

[10] New Jersey Company Pleads Guilty and Agrees to Restitution and Civil Penalty for Failing to Report Dangerous Air Conditioners, Dept of Justice Press Release (Aug. 5, 2025); found at: https://www.justice.gov/opa/pr/new-jersey-company-pleads-guilty-and-agrees-restitution-and-civil-penalty-failing-report.

[11] *See* Statement of Acting Chairman Peter A. Feldman, *supra*.

[12] See, e.g., Evaluation of Corporate Compliance Programs, US Department of Justice Criminal Division (Updated Sept. 2024); found at: https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=.

Well-defined programs

Prosecutors begin with risk assessment. They assess how a company identifies and defines its risk profile, including risks associated with foreign manufacturing, testing integrity, certification accuracy, and supply chain documentation. A defensible program must demonstrate that compliance controls are tailored to the company's product mix, sourcing model, and regulatory exposure. For retailers and importers of CPSC-regulated goods, this includes processes for validating test reports, confirming certificate accuracy, ensuring supplier qualification, and maintaining documentation continuity across the product lifecycle. DOJ guidance also emphasizes whether the program evolves over time in response to enforcement trends, industry developments, and lessons learned—both internal and external—and whether emerging risks are actively identified and addressed.

Good-Faith Implementation and Resourcing

Even a well-designed program may be ineffective if it lacks adequate authority, funding, or technological support. Prosecutors are instructed to distinguish between a "paper program" and one that is meaningfully implemented, tested, and revised. This includes evaluating whether compliance personnel have sufficient access to relevant operational and supply chain data to monitor testing compliance, certification status, and import documentation in real time. DOJ guidance also asks whether the resources devoted to compliance—including technology and data analytics capabilities—are proportionate to the company's size and risk profile. In an environment shaped by electronic filing and increased regulatory transparency, continuous access to accurate compliance data is not aspirational; it is expected.

Effectiveness in Practice

Finally, prosecutors assess whether the compliance program works—both at the time of any alleged violation and at the time of a charging decision. Hallmarks of effectiveness include proactive monitoring, periodic testing of controls, documented corrective action processes, and demonstrable program improvement over time. Companies that can show early identification of documentation gaps, testing deficiencies, or supplier noncompliance—and prompt remediation—are better positioned to receive prosecutorial credit. Static policies and retrospective audits are insufficient; regulators expect measurable, data-driven oversight.

Core expectations therefore include:

- A clearly articulated, risk-based compliance methodology
- Continuous access to relevant testing, certification, and import data
- Proactive monitoring and validation of product compliance controls
- Documented remediation and corrective action processes
- Ongoing program evolution informed by enforcement trends and lessons learned
- Proportionate allocation of financial, technological, and human resources

For retailers and importers, these standards carry particular weight. The importation of regulated consumer goods—especially in a regime of electronic filing and enhanced data visibility—creates concentrated regulatory exposure at the point of entry into U.S. commerce.

Why Traditional Compliance Models Break Down

Legacy compliance frameworks were built for relatively stable supply chains, manageable volumes of inventory, and retrospective corrective action—not real-time compliance verification and digital reporting at scale. That model becomes structurally inadequate in modern retail and high-volume import environments characterized by:

- Fragmented documentation storage
- Manual certification tracking
- Limited supplier visibility
- Reactive error correction
- Version control challenges
- Inconsistent audit readiness

At scale, manual verification is neither operationally feasible nor defensible—traditional sampling methods and periodic audits inevitably create blind spots. Those blind spots are increasingly problematic in a regulatory environment that emphasizes continuous data access, proactive monitoring, and real-time regulator visibility into import compliance. Sampling may have been tolerable in a lower-volume, inspection-driven enforcement model; it is far less sustainable under frameworks that assume systemic visibility and immediate accountability.

Fragmented systems compound the problem. When testing records, certifications, supplier documentation, and import data reside in disconnected platforms, organizations lack the ability to track product compliance and provide the documentation necessary for entries to clear customs without delay. Compliance teams are forced to reconcile information manually, slowing response times and increasing the likelihood of shipment holds and increased inspections.

Traditional models were designed for a different era. Modern regulatory expectations demand infrastructure capable of persistent monitoring, documentation integrity, and systemic visibility to product data.

A Modern AI-Enabled Compliance Architecture for Importers and Retailers

An effective compliance program integrates automation, analytics, and workflow orchestration into a unified system. Core capabilities include:

1. Intelligent Supplier Qualification & Documentation Verification

AI-supported workflows validate supplier certifications, testing credentials, and regulatory eligibility. Continuous monitoring flags documentation gaps before products enter commerce.

2. Automated Testing & Certification Data Management

Structured ingestion and validation of laboratory reports and certifications ensure data integrity, version control, and traceability to specific SKUs.

3. Regulatory Mapping & Rule Integration

Embedded logic aligns product data with applicable safety standards, reducing interpretation errors and ensuring consistent compliance decisions.

4. Lifecycle Monitoring & Data Integrity Controls

Continuous system checks detect anomalies, expired documentation, or compliance drift across supplier and product portfolios.

5. Evidence Management & Audit Readiness

Automated documentation capture preserves certification histories and decision logs, creating defensible audit trails aligned with enforcement expectations.

6. Adaptive Learning & Continuous Improvement

Feedback loops incorporate operational insights and regulatory developments to refine compliance controls over time.

Together, these capabilities establish a closed-loop compliance ecosystem capable of supporting high-volume import and retail operations while maintaining regulatory discipline.

Operational and Strategic Benefits

AI-enabled compliance infrastructure delivers measurable value to import and retail organizations:

- Reduced shipment disruption and litigation risk
- Stronger documentation integrity
- Early detection of compliance gaps
- Improved supplier governance
- Scalable import operations
- Enhanced audit readiness
- Regulatory confidence

Compliance becomes an operational enabler—supporting growth while protecting market access.

External Systems as a Compliance Risk Control

Relying on an independent third-party provider to conduct risk assessments and support core compliance functions—particularly through AI-enabled systems—can be a powerful governance decision, not merely an operational one. Separating compliance systems from internal commercial priorities reduces both the risk and the perception that business pressures could influence compliance judgments. That structural independence strengthens credibility with regulators, courts, auditors, and stakeholders who increasingly scrutinize whether compliance programs are designed to function objectively and without competing incentives. External expertise combined with purpose-built technology delivers consistency, transparency, and data-driven rigor that is difficult to achieve through internally managed processes alone. In an environment where the defensibility of compliance decisions is as important as the decisions themselves, organizations that embed independent compliance infrastructure position themselves to demonstrate integrity, accountability, and proactive governance—advantages that directly support regulatory confidence and long-term operational stability.

Conclusion: Compliance as Operational Infrastructure

Retailers and importers of regulated consumer goods are facing a decisive regulatory transformation. The CPSC's e-Filing Rule is not simply a procedural change—it signals a fundamental shift toward continuous, data-driven verification of product safety and certification integrity. Product compliance can no longer function as a retrospective exercise supported by fragmented documentation or manual review; it is becoming an operational requirement that regulators can evaluate in near real time. Organizations that fail to modernize their compliance systems face increasing exposure to shipment disruption, enforcement action, and reputational harm as regulators gain greater visibility into importer and retailer practices. By contrast, companies that implement integrated, intelligent compliance infrastructure position themselves to validate testing and certification data in real time, maintain defensible audit trails, monitor supplier performance, and respond quickly to emerging risks. In an environment where regulators expect demonstrable readiness and systemic accountability, treating compliance as core operational infrastructure is no longer optional—it is essential to protecting market access, sustaining supply chain velocity, and preserving organizational credibility. The urgency is clear: modern compliance capability must be built now, before regulatory expectations become operational consequences.

Call to Action

The importation and retail sale of consumer products unsupported by disciplined compliance infrastructure creates preventable safety, regulatory, legal, and operational risk. As electronic verification becomes central to how product compliance is assessed, unmanaged documentation processes and reactive oversight can quickly translate into shipment delays, enforcement actions, lawsuits, and loss of brand value. Organizations that act now to modernize their compliance architecture position themselves to maintain continuous visibility into testing and certification data, strengthen supplier accountability, and demonstrate audit-ready governance when it matters most. AI-enabled compliance infrastructure provides the scale, consistency, and defensibility required in

today's regulatory environment. The transition to modern compliance systems is not a future consideration—it is an immediate operational priority. The organizations that move decisively will protect market access, preserve supply chain continuity, and reinforce trust.

The time to deploy those capabilities is now. We can help.

About the Author:

Kenneth R. Hinson (Ken) is President of ICW North America and a former Executive Director of the U.S. Consumer Product Safety Commission, where he managed the agency's compliance, import surveillance, and hazard reduction operations. Over the course of nearly 25 years, he has led regulatory and compliance functions at some of the world's largest retail organizations, including Walmart Inc. and QVC Group. His experience spans enforcement oversight, enterprise risk assessment, and the design of global product compliance programs capable of withstanding regulatory scrutiny. He advises retailers, importers, manufacturers, and marketplace operators on integrating modern compliance infrastructure that is operationally embedded and defensible in evolving enforcement environments.

ICW provides AI-powered compliance solutions trusted by Fortune 500 retailers to manage over 10 million product SKUs annually.

Our team comprises former CPSC senior officials, customs attorneys, supply chain data scientists and product compliance experts dedicated to bridging the gap between regulatory complexity and operational reality.