White Paper

Why Third-Party Marketplaces Must Invest in an AI-Powered End-to-End Product Safety & Compliance Solution

Executive Summary

Third-party marketplace growth has reshaped retail at unprecedented speed. Alongside that expansion comes a regulatory and litigation environment that increasingly treats marketplace operators as active participants in product distribution—not neutral intermediaries. Enforcement agencies are intensifying scrutiny, courts are reexamining liability doctrines, and government prosecutors expect compliance programs to be risk-driven, data-enabled, and demonstrably effective.

Traditional compliance programs—periodic audits, decentralized documentation, and siloed systems—cannot keep pace with the scale and velocity of modern marketplace ecosystems. Compliance operators must instead deploy intelligent, integrated infrastructure capable of continuous monitoring, seller verification, regulatory alignment, and audit-ready documentation.

This paper explores the increasing risks faced by marketplaces and outlines a modern compliance architecture designed specifically for marketplace environments: an AI-enabled, end-to-end framework that integrates product safety validation, seller oversight, regulatory intelligence, lifecycle monitoring, and adaptive risk management. Such an architecture transforms compliance from a reactive obligation into a strategic operational capability that protects growth, strengthens governance, and reduces exposure.

Marketplace Expansion: Growth and Structural Risk

Marketplace platforms enable rapid assortment scaling, global seller participation, and capital-efficient expansion for retailers. Yet this model inherently distributes operational control across thousands—sometimes millions—of independent sellers. Many online marketplaces also function as more than passive platforms for third-party sales. They increasingly provide fulfillment services, listing governance, customer engagement, and other services ancillary to the sale of products. As the lines between seller and platform host continue to blur, complex liability questions emerge—including an ongoing legal dispute involving the U.S. Consumer Product Safety Commission (CPSC) regarding whether marketplace operators qualify as “distributors” under the Consumer Product Safety Act.[1] The result is a risk profile that is dynamic, cross-jurisdictional, unpredictable, and difficult to manage effectively without structured, technology-enabled oversight.

[1] *See*, CPSC Issues Final Order to Amazon.com Outlining Remediation Plans for Hazardous Products; found at: https://www.cpsc.gov/Newsroom/News-Releases/2025/CPSC-Issues-Final-Order-to-Amazon-com-Outlining-Remediation-Plans-for-Hazardous-Products.

Marketplace operators increasingly face exposure arising from:

- Product safety defects
- Regulatory non-compliance
- Restricted or prohibited goods
- Counterfeit or gray-market items
- Cross-border compliance gaps
- Seller identity opacity
- Documentation deficiencies

Regulators and courts increasingly view marketplaces as uniquely positioned to manage these risks, even when the marketplace host is not the direct seller. Incidents involving unsafe or non-compliant products can trigger recalls, enforcement actions, litigation, and reputational harm that affects the entire platform ecosystem and brand.

Aggressive Enforcement Environment

The enforcement posture surrounding consumer product safety has become more assertive, particularly regarding imported goods and third-party sellers. The CPSC has both articulated and demonstrated an increasing emphasis on inspections, recalls, and takedown initiatives, signaling heightened expectations that marketplace operators maintain proactive safeguards. In 2025, the CPSC issued more than 88,250 takedown notices of recalled and violative products from online marketplaces—an increase of ~50% over 2024.[2] Also 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. For marketplace operators, this shift materially changes the risk equation. Enforcement exposure is no longer driven solely by the scale of harm or volume of distribution; even limited sales of a noncompliant product can prompt regulatory

---

[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*.

action. In this environment, the assumption that low probability equates to low risk is increasingly untenable.

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 marketplaces, this underscores a critical reality—regulatory compliance itself has become an independent enforcement priority. Verification of conformity with applicable safety rules becomes a prerequisite for listing; not relegated to a remedial exercise after a problem surfaces.

The geographic concentration of recalls further reinforces this enforcement posture and the corresponding risk exposure for marketplaces. In 2025, 71% of recalled products were manufactured in China, reflecting the Commission's heightened scrutiny of imported consumer goods.[8] As the volume of foreign-manufactured products on a marketplace increases, so too does the platform's potential enforcement risk. Cross-border marketplace participation adds another layer of complexity, requiring platform hosts to reconcile differing product standards, documentation requirements, and jurisdictional obligations while maintaining real-time oversight of seller activity.

Collectively, these factors point toward heightened regulatory scrutiny of products sold through third-party marketplaces—particularly those that are imported. Effective compliance now requires:

- Continuous product and seller verification
- Embedded regulatory intelligence
- Automated anomaly detection
- Rapid remediation workflows
- Audit-ready documentation

Manual oversight cannot scale to meet these demands, and the 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

---

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

in penalties and restitution against companies the agency determined was violating U.S. product safety laws.[11]

Judicial and Liability Trends

Historically, marketplace hosts relied on legal doctrines that limited liability for third-party sellers, such as Section 230 of the Communications Decency Act.[12] Consequently, marketplaces often demurred on vetting third-party listings for compliance with applicable product laws and regulations in part for fear of assuming liability where there previously was none. That protective landscape is shifting. Courts are increasingly recognizing that marketplace operators exercise meaningful control over third-party transactions, including payment processing, fulfillment logistics, listing governance, and customer engagement.[13] Compounding the problem, regulators face increasing difficulty compelling foreign sellers to cooperate with recall demands and will look increasingly toward marketplace hosts for the solution. Where third-party sellers are unreachable or offshore, platforms are increasingly being viewed as the domestic risk gatekeepers.

The practical consequence is a widening interpretation of marketplace responsibility in product safety disputes. Regulatory findings and evolving judicial reasoning indicate that liability exposure is no longer theoretical—it is an operational reality requiring systemic risk controls.

Prosecutorial Standards for Modern Compliance Programs

The U.S. Department of Justice evaluates corporate compliance programs through a structured and rigorous framework.[14] Prosecutors are instructed to ask three fundamental 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 questions move beyond written policies and examine whether compliance systems are operational, risk-informed, data-enabled, and capable of detecting and addressing misconduct before it escalates.

Well-defined programs

Prosecutors begin with risk assessment. They evaluate how a company identifies, assesses, and defines its risk profile; whether compliance controls are tailored to the company's specific business model and regulatory environment; and whether resources are deployed proportionately to higher-risk activities. A defensible program must demonstrate that it has evolved over time in response to changing risks, industry developments, and lessons learned—both internally and from peer

---

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., Section 230: An Overview, Report by Congressional Research Services (Jan. 4, 2024); found at: https://www.congress.gov/crs-product/R46751.

[13] See, e.g., Oberdorf v. Amazon.com Inc, No. 18-1041 (3d Cir. 2019); found at: https://law.justia.com/cases/federal/appellate-courts/ca3/18-1041/18-1041-2019-07-03.html; see also, Bolger v. Amazon.com, LLC, 53 Cal.App.5th 431 (2020); found at: https://law.justia.com/cases/california/court-of-appeal/2020/d075738.html.

[14] 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=.

organizations. Regulators also assess whether companies have processes in place to identify and manage emerging risks, rather than relying on static "snapshot" reviews.

Good-Faith Implementation and Resourcing

Even a well-designed program may fail if it is under-resourced or lacks autonomy. DOJ guidance directs prosecutors to distinguish between a "paper program" and one that is implemented, reviewed, tested, and revised in practice. This includes examining whether compliance personnel have sufficient authority, funding, and technological tools to conduct auditing, documentation review, and risk analysis effectively. Prosecutors also compare the technology and resources devoted to risk mitigation with those deployed for revenue generation, asking whether compliance capabilities are proportionate to the organization's size, structure, and risk profile. Continuous access to relevant operational data—and appropriate use of data analytics to monitor transactions and controls—is now a core expectation.

Effectiveness in Practice

Finally, prosecutors assess whether the compliance program works. This evaluation occurs both at the time of any alleged misconduct and at the time of charging decisions. Hallmarks of effectiveness include continuous improvement, periodic testing, proactive monitoring, documented remediation processes, and the ability to identify issues at the earliest possible stage. Programs that demonstrate transparency, measurable performance indicators, and documented adaptation to emerging risks are more likely to receive credit.

Core expectations therefore include:

- A clearly articulated, risk-based methodology
- Continuous access to relevant compliance data
- Proactive monitoring and testing of controls
- Documented remediation and corrective action processes
- Ongoing program evolution based on lessons learned
- Proportionate deployment of financial, technological, and human resources

For marketplace operators, these standards have direct implications. The distributed, high-volume nature of third-party selling creates identifiable risk concentrations, including product safety, cross-border compliance, and seller oversight. DOJ expectations require that these risks be addressed through structured systems embedded within operational workflows, supported by data visibility and automation. Compliance cannot be confined to policy documentation or reactive enforcement. It must be demonstrably integrated into listing controls, seller onboarding, monitoring mechanisms, and corrective processes in a manner capable of standing up to prosecutorial scrutiny.

Why Traditional Compliance Models Break Down

Legacy compliance frameworks were built for relatively stable supply chains, predictable product lifecycles, and manageable volumes of inventory. They rely heavily on periodic audits, manual documentation review, and retrospective corrective action. That model becomes structurally inadequate in modern marketplace and high-volume retail environments characterized by:

- High-velocity product onboarding
- Distributed seller accountability
- Cross-border regulatory variability
- Continuous catalog churn
- Large-scale documentation management

At scale, manual verification is neither operationally feasible nor defensible. When platforms manage millions—and in some cases billions—of SKUs across global sellers and suppliers, 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 early detection. 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 real-time accountability.

Fragmented systems compound the problem. When testing records, certifications, supplier documentation, and listing data reside in disconnected platforms, organizations lack unified risk visibility. Compliance teams are forced to reconcile information manually, slowing response times and increasing the likelihood that noncompliant products enter and remain in commerce.

Reactive processes are equally vulnerable, and programs that rely on static policies, after-the-fact audits, or episodic remediation are increasingly difficult to defend. In a high-volume, cross-border environment, compliance must operate continuously and at scale; otherwise, risk accumulates faster than oversight mechanisms can respond.

Traditional models were designed for a different era. Modern regulatory expectations demand infrastructure capable of persistent monitoring, documentation integrity, and systemic risk visibility across the full product lifecycle.

A Modern AI-Enabled Marketplace Compliance Architecture

An effective compliance framework for marketplace environments combines automation, analytics, and workflow orchestration across the entire product lifecycle. The architecture of an effective compliance program incorporates several core capabilities:

1. Intelligent Seller Qualification & Identity Assurance

AI-supported onboarding workflows validate seller credentials, documentation, and jurisdictional eligibility. Continuous monitoring detects anomalies, risk signals, or documentation gaps, enabling proactive intervention before listings go live.

2. Automated Product Safety & Regulatory Validation

Machine-driven screening evaluates listings against safety standards, labeling requirements, restricted product criteria, and jurisdiction-specific regulations. Embedded rule engines translate regulatory complexity into operational controls.

3. Compliance Knowledge Integration

Centralized regulatory intelligence continuously maps evolving safety standards, import restrictions, and documentation requirements into actionable system logic.

4. Lifecycle Monitoring & Risk Detection

Continuous scanning identifies emerging risks, product anomalies, seller behavior patterns, and compliance drift. AI models prioritize alerts based on risk severity, enabling efficient remediation workflows.

5. Evidence Management & Audit Readiness

Automated documentation capture preserves verification records, product certifications, seller attestations, and review histories. This creates defensible audit trails aligned with enforcement expectations.

6. Adaptive Learning & Continuous Improvement

Feedback loops integrate incident data, enforcement trends, and operational insights to refine detection models and compliance controls over time.

Together, these capabilities establish a closed-loop compliance ecosystem capable of operating at marketplace scale while maintaining governance rigor.

Operational and Strategic Benefits

An AI-enabled compliance infrastructure delivers measurable enterprise value:

- Reduced litigation and enforcement exposure
- Early detection of unsafe or non-compliant products
- Strengthened seller governance
- Scalable cross-border operations
- Improved documentation integrity

- Enhanced consumer trust
- Operational efficiency

Critically, compliance becomes a growth enabler—not a constraint—supporting expansion while protecting organizational resilience.

External Architecture as a Compliance Risk Control

Leveraging an independent third-party provider to manage product risk assessments and other core compliance functions—particularly through AI-enabled systems—can materially strengthen an organization's governance framework. External compliance infrastructure introduces structural separation between commercial decision-making and compliance evaluation, helping ensure that risk judgments are guided by objective standards rather than internal business pressures. This independence not only improves consistency and technical rigor, but also enhances credibility with regulators, courts, auditors, and stakeholders who increasingly evaluate whether compliance programs are designed to operate free from competing incentives. Third-party expertise, combined with purpose-built technology, allows organizations to demonstrate that compliance oversight is systematic, data-driven, and insulated from operational bias. In an enforcement environment that places growing emphasis on program integrity and defensibility, relying on independent compliance infrastructure is as much a governance decision as it is an operational one—reinforcing transparency, accountability, and long-term resilience.

Conclusion: Compliance as Marketplace Infrastructure

Third-party marketplace operators are facing a decisive shift in how product safety and compliance responsibility is evaluated. Evolving regulatory expectations and liability standards are no longer treating platforms as passive intermediaries; they reflect a broader movement toward continuous, data-driven accountability for product safety, seller oversight, and documentation integrity. Marketplace compliance can no longer function as a retrospective exercise supported by fragmented controls or manual review—it is becoming an operational requirement subject to increasing regulatory and legal scrutiny. Organizations that fail to modernize their compliance systems face growing exposure to enforcement action, litigation, platform disruption, and reputational harm as regulators and courts gain greater visibility into marketplace practices. By contrast, companies that implement integrated, intelligent compliance infrastructure position themselves to validate product and seller data in real time, maintain defensible audit trails, monitor ecosystem risk, and respond quickly to emerging safety concerns. In an environment where authorities expect demonstrable readiness and systemic accountability, treating compliance as core operational infrastructure is no longer optional—it is essential to protecting platform integrity, sustaining growth, and preserving organizational credibility. The urgency is clear: modern compliance capability must be built now, before escalating expectations become operational consequences.

Call to Action

Marketplace growth unsupported by disciplined compliance infrastructure creates preventable safety, regulatory, legal, and operational risk. As oversight becomes increasingly data-driven and liability standards continue to evolve, unmanaged seller controls, fragmented documentation, and reactive compliance processes can quickly translate into enforcement exposure, litigation, consumer harm, and erosion of platform trust. Organizations that act now to modernize their compliance architecture position themselves to maintain continuous visibility into product and seller risk, strengthen oversight mechanisms, and demonstrate audit-ready governance when it matters most. AI-enabled product safety and compliance infrastructure provides the scale, consistency, and defensibility required in today's enforcement environment. The transition to modern marketplace compliance systems is not a future consideration—it is an immediate operational priority. Platforms that move decisively will protect ecosystem integrity, sustain growth, and reinforce stakeholder confidence.

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.