Testimony of:

Daniel Castro
President
Information Technology and Innovation Foundation

Before the:

House Subcommittee on Commerce, Manufacturing, and Trade

Hearing on:

"Legislative Proposals to Strengthen Consumer Protection in a Changing Marketplace"

July 22, 2026
212 Rayburn House Office Building
Washington, DC

CONTENTS

INTRODUCTION AND SUMMARY

Chairman Bilirakis, Vice Chairman Fulcher, Ranking Member Schakowsky, and members of the subcommittee, thank you for the opportunity to appear before you today to discuss opportunities to protect American consumers from dangerous goods, improve transparency in markets, and reduce fraud.

My name is Daniel Castro, and I am president of the Information Technology and Innovation Foundation (ITIF), an independent, nonprofit, nonpartisan think tank dedicated to advancing technological innovation and productivity.

Online marketplaces have transformed commerce by expanding consumer choice, lowering prices, and enabling millions of businesses to reach customers nationwide. These platforms have become an essential part of the U.S. economy, and policymakers should preserve the innovation and competition they create.

But those benefits depend on consumer trust. Americans should not have to wonder whether the products they purchase are authentic, safe, or accurately described, or whether the sellers offering them are legitimate. Likewise, honest businesses should not have to compete against sellers that rely on deception, evade accountability, or repeatedly offer counterfeit, unsafe, or fraudulent products. Effective marketplace governance protects consumers, rewards responsible businesses, and strengthens confidence in digital commerce.

The challenge is that not all marketplaces have invested equally in those protections. ITIF's research finds significant differences in how major online marketplaces verify sellers, detect counterfeit and unsafe products, remove repeat offenders, and promote transparency. These differences are especially pronounced among several major Chinese online marketplaces serving U.S. consumers. Because these platforms reach tens of millions of Americans, shortcomings in marketplace governance can expose consumers to greater risks of fraud, counterfeit products, and unsafe goods. Existing enforcement mechanisms have not created sufficient incentives for these platforms to improve their practices.

Congress has an opportunity to strengthen consumer protection while preserving the benefits of digital commerce. No marketplace can eliminate every counterfeit product or fraudulent seller. But every marketplace serving American consumers should meet reasonable expectations for seller accountability, transparency, and effective action against harmful conduct.

My testimony makes four principal points:

- First, counterfeit and unsafe products pose significant consumer protection risks. Consumers purchasing everyday goods deserve confidence that the products they receive are authentic, safe, and comply with applicable standards.
- Second, several major Chinese online marketplaces compete in part by investing less in marketplace governance than leading U.S. platforms, resulting in weaker seller verification, less effective enforcement against repeat offenders, slower responses to dangerous products, and lower levels of transparency.
- Third, existing enforcement tools remain largely reactive. Congress should complement them by creating stronger incentives for marketplaces to prevent harmful conduct before it reaches consumers.
- Finally, Congress should evaluate proposals affecting digital marketplaces according to four principles: preventing harm, strengthening transparency, preserving incentives to innovate in consumer protection, and holding all marketplaces serving American consumers to comparable standards.

I. CONSUMER PROTECTION DEPENDS ON MARKETPLACE GOVERNANCE

Online marketplaces have transformed commerce by connecting buyers and third-party sellers at a scale that was previously impossible. Unlike traditional online retailers, which generally purchase inventory and sell products directly to consumers, online marketplaces facilitate transactions between independent sellers and buyers. This model expands consumer choice, lowers prices through greater competition, and allows entrepreneurs and small businesses to reach customers around the world. It has become one of the defining innovations of the digital economy.

The marketplace model also presents different policy questions. Because marketplaces act as intermediaries rather than retailers, they do not exercise the same level of control over every product offered for sale. Third-party sellers may operate from anywhere in the world, may never handle products through the marketplace itself, and in some cases may fall outside the practical reach of U.S. regulators or courts. For these reasons, policymakers have debated whether and when online marketplaces should bear legal responsibility for defective or counterfeit products sold by third-party sellers.

That debate is important, but it is not the focus of my testimony. The more immediate question is how marketplaces choose to govern their platforms. Many leading U.S. marketplaces have voluntarily invested in seller verification, counterfeit detection, product recall systems, customer guarantees, dispute resolution, and other consumer protections that exceed their legal obligations. These investments require significant resources, but they also represent an important form of competition. Marketplaces increasingly compete not only on price and selection, but also on the quality of the protections they offer buyers and sellers.

ITIF's research finds that several major Chinese online marketplaces serving U.S. consumers have made different choices. While they compete aggressively on price and selection, they generally provide weaker marketplace governance than leading U.S. platforms. The result is not that every product offered on these marketplaces is unsafe or counterfeit. Rather, consumers appear to face a greater risk of encountering fraudulent sellers, counterfeit products, and dangerous goods than they would on marketplaces that invest more heavily in consumer protection.

Counterfeit products illustrate the problem. Many people think of counterfeits primarily as an intellectual property issue that harms brand owners. But counterfeit goods also create direct consumer protection risks. A counterfeit cosmetic may contain unsafe ingredients. A counterfeit phone charger may overheat or catch fire. Counterfeit medications, children's products, automotive parts, and pet products may fail to meet basic safety standards. Consumers viewing an online listing often have no practical way to distinguish a genuine product from a sophisticated counterfeit before making a purchase.

To better understand the scope of the problem, ITIF examined listings on several major Chinese online marketplaces serving U.S. consumers.[1] Researchers identified products that appeared suspicious based on pricing, seller information, product descriptions, images, and other indicators. After purchasing the products, ITIF sought to determine whether they were authentic. The investigation confirmed that consumers could readily purchase likely counterfeit products across multiple categories, including apparel, cosmetics, toys, over-the-counter medicines, and household goods.

Some of the findings raise serious consumer safety concerns. In one case, ITIF purchased what appeared to be dog treats from the U.K.-based pet food company NutriPaw. The packaging contained obvious warning signs, including multiple spelling errors and a misspelled brand name. The barcode corresponded to an unrelated product rather than the advertised item. After reviewing the product, NutriPaw confirmed that it was counterfeit and informed ITIF that it had previously received a report from a customer whose dog became severely ill after consuming similar fake treats.

ITIF also purchased a product marketed as a cold medicine that closely resembled Theraflu Nighttime Severe Cold Relief Powder. After reviewing photographs and product information, the manufacturer concluded that the product was most likely counterfeit. Counterfeit over-the-counter medicines present particularly serious risks because consumers may unknowingly rely on products that contain the wrong ingredients, incorrect dosages, contaminants, or no active ingredients at all.

After ITIF published its report, Temu removed nearly all of the specific products and sellers identified in it. However, follow-up research found that additional over-the-counter medicines continued to appear on the platform, sometimes listed under unrelated product categories. This pattern suggests that removing individual listings, while necessary, is not sufficient if marketplaces do not also identify and prevent repeat offenders or detect similar listings before they reach consumers.

Counterfeits represent only one manifestation of a broader challenge. The same conditions that permit counterfeit products to appear on a marketplace can also allow recalled products, products that fail to comply with applicable safety requirements, and other fraudulent or deceptive listings to reach consumers. For example, testing has found that shoes sold on popular Chinese e-commerce platforms contain unsafe levels of toxic substances.[2] The issue is therefore not simply counterfeit goods, but rather the overall effectiveness of marketplace governance.

Here too ITIF found meaningful differences between major U.S. and Chinese online marketplaces. Leading U.S. marketplaces generally have invested heavily in seller verification, trust-and-safety systems, counterfeit detection, recall management, customer protections, and dispute resolution. These capabilities require sophisticated technology, substantial operational investment, and ongoing collaboration with manufacturers, rights holders, and government agencies. They also provide meaningful benefits to consumers.

Several major Chinese marketplaces serving U.S. consumers appear to have invested less heavily in these capabilities. As a result, consumers shopping on these platforms often shoulder greater responsibility for evaluating unfamiliar sellers, identifying counterfeit listings, and avoiding unsafe products—frequently without realizing that the protections available to them differ from those offered by leading U.S. marketplaces.

II. SOME CHINESE PLATFORMS GAIN A COMPETITIVE ADVANTAGE BY INVESTING LESS IN MARKETPLACE GOVERNANCE

The evidence presented in the previous section points to a broader conclusion. The differences between leading U.S. and Chinese online marketplaces do not primarily reflect differences in technology or engineering capability. They reflect different business models and different competitive choices.

Over the past two decades, leading U.S. online marketplaces have invested heavily in technologies and business processes that make digital commerce safer and more reliable. These investments include artificial intelligence (AI) systems that detect fraudulent listings, seller reputation systems, identity verification, counterfeit detection tools, product traceability, recall management systems, customer guarantees, and large trust-and-safety teams. Marketplace governance has become an important area of innovation in its own right.

These capabilities require significant investment. They depend on sophisticated software, engineering talent, operational expertise, and ongoing collaboration with manufacturers, rights holders, and government agencies. They also create real value for consumers by reducing fraud, improving transparency, and making digital commerce more dependable.

ITIF's research suggests that several major Chinese online marketplaces have pursued a different competitive strategy. Rather than investing as heavily in these capabilities, they have emphasized rapid seller onboarding, expansive product catalogs, and very low prices. Those choices have helped these platforms grow quickly, but they have also created conditions in which counterfeit products, unsafe goods, and fraudulent sellers can remain active longer and reach more consumers.

Importantly, this does not appear to reflect technological limitations. These foreign companies possess world-class engineering talent and sophisticated technical capabilities. The relevant question is not whether they can build stronger consumer protections, but whether they have sufficient incentives to do so for products sold to American consumers.

China's policy environment reinforces these incentives. As ITIF has documented, Chinese online marketplaces operate within an ecosystem in which counterfeit goods intended for foreign markets continue to circulate at significant scale. China committed in the Phase One trade agreement to strengthen enforcement against counterfeit goods, including by taking effective action against e-commerce platforms that fail to address infringement and by increasing enforcement against counterfeit products that pose health and safety risks.[3] Yet ITIF's research indicates that these commitments have not produced adequate protections for American consumers purchasing through major Chinese online marketplaces.

Congress should also consider the broader competitive landscape. The United States maintains one of the world's most open digital markets. Major Chinese online marketplaces enjoy broad access to American consumers. By contrast, many leading U.S. online marketplaces have little or no comparable access to China's domestic market because of longstanding restrictions on foreign digital services. China blocks many U.S. digital platforms outright through its Internet controls, and companies seeking to operate legally in China must navigate stringent requirements for government-approved licensing, real-name identity verification, data localization, and compliance with extensive censorship and cybersecurity rules. As a result, many leading U.S. online marketplaces either cannot operate in China or would have to fundamentally redesign their business models and technical infrastructure to do so.

The same pattern appears in other digital marketplaces. A comparative study of Chinese and U.S. mobile app stores found that leading U.S. app stores employed more rigorous app review processes, distributed significantly fewer malicious applications, and removed harmful apps more consistently than their Chinese counterparts.[4]

Competition among digital marketplaces drives innovation and creates value for consumers. But the basis of that competition matters. Firms should compete by building better technologies, offering better services, and delivering stronger consumer protections—not by shifting more of the costs of fraud and unsafe products onto consumers.

III. REACTIVE ENFORCEMENT ALONE WILL NOT PROTECT CONSUMERS

Federal agencies play an essential role in protecting consumers from dangerous products, counterfeit goods, and online fraud. U.S. Customs and Border Protection intercepts counterfeit imports, the Consumer Product Safety Commission identifies hazardous consumer products, the Federal Trade Commission combats deceptive practices, and the Office of the U.S. Trade Representative identifies foreign markets that facilitate counterfeiting and piracy. These efforts make meaningful contributions to consumer protection.

The challenge is that today's enforcement framework remains largely reactive. Agencies often identify dangerous products only after they have entered the marketplace, reached consumers, or generated complaints. Removing individual products remains important, but it does not address the marketplace practices that allow repeat offenders to return under new identities or relist substantially similar products.

ITIF's research illustrates this challenge. After identifying likely counterfeit products and notifying the relevant marketplaces, some platforms removed the specific listings identified in the report. Yet researchers continued to find substantially similar products available for purchase, including additional over-the-counter medicines that appeared under unrelated product categories. These findings suggest that some platforms continue to rely primarily on responding to individual reports rather than systematically identifying repeat offenders or preventing similar listings from appearing in the first place.

Independent evidence points to the same conclusion. After the Consumer Product Safety Commission warned consumers about hazardous products sold through online marketplaces, leading U.S. marketplaces had removed the identified products from sale. Several major Chinese marketplaces, however, continued offering the same products or substantially identical alternatives. Likewise, independent testing by The Toy Association found that nearly 90 percent of toys purchased from two leading Chinese online marketplaces presented significant safety concerns, with more than 70 percent failing at least one laboratory safety test.[5] These findings reinforce the conclusion that product safety concerns on these platforms are systemic rather than isolated incidents.

Regulators have also begun responding directly to marketplace practices. The Federal Trade Commission recently penalized Temu for violating the INFORM Consumers Act after determining that it had not adequately complied with statutory requirements designed to protect consumers from stolen, counterfeit, or unsafe goods.[6] That enforcement action demonstrates both the importance of existing consumer protection laws and the need for continued vigilance as online marketplaces evolve.

The Office of the U.S. Trade Representative's Notorious Markets process illustrates another limitation. ITIF submitted original evidence documenting the sale of counterfeit products through several major Chinese online marketplaces and recommended that USTR designate them as notorious markets.[7] Despite this evidence, the marketplaces were not included in USTR's final report.[8] Regardless of the reasons for that decision, the outcome underscores a broader point: existing mechanisms have not created sufficient incentives for meaningful improvements in marketplace governance.

Effective enforcement also depends on transparency. Researchers, manufacturers, regulators, and consumers cannot identify harmful conduct if marketplace practices make suspicious listings difficult to discover or obscure the identities of repeat sellers. Greater transparency strengthens accountability by enabling independent parties to identify patterns of fraud, verify compliance, and alert marketplaces and regulators to emerging risks before they become widespread.

Congress should build on existing enforcement efforts by placing greater emphasis on prevention. Marketplaces possess information and technical capabilities that government agencies often do not. Better seller verification, stronger enforcement against repeat offenders, improved marketplace transparency, and closer cooperation with regulators can prevent more unsafe and fraudulent products from reaching consumers while preserving the benefits of digital commerce.

IV. CONGRESS SHOULD STRENGTHEN CONSUMER PROTECTION WITHOUT UNDERMINING INNOVATION

The evidence presented in this testimony points to four principles that should guide Congress as it considers legislation affecting digital marketplaces.

First, focus on preventing harm rather than responding after the fact. Government agencies will always play an important enforcement role, but marketplaces possess information and technical capabilities that regulators often do not. Congress should encourage marketplaces to identify high-risk sellers, detect fraudulent listings, and remove repeat offenders before counterfeit, unsafe, or fraudulent products reach consumers.

Second, strengthen transparency and information sharing. Effective enforcement depends on timely access to information. Consumers deserve to know who is selling products, rights holders need better tools to identify counterfeit networks, and regulators should be able to work more effectively with marketplaces and legitimate businesses to identify repeat offenders. Congress should support greater information sharing across government and the private sector to disrupt counterfeit supply chains rather than addressing violations one shipment at a time.

Third, preserve incentives to innovate in consumer protection. Marketplace governance has become an important area of technological innovation. AI, identity verification, fraud detection, product traceability, and trust-and-safety systems all make digital markets safer and more reliable. Congress should establish clear expectations for marketplace integrity while allowing firms to continue innovating in how they meet those expectations.

Fourth, hold all marketplaces serving American consumers to comparable standards. The United States has one of the world's most open digital markets, while many leading U.S. online marketplaces remain unavailable or severely restricted in China because of longstanding barriers to foreign digital services. The United States benefits from open markets, but companies that seek access to American consumers should meet reasonable expectations for transparency, seller accountability, and consumer protection regardless of where they are headquartered.

These principles support both consumer protection and American competitiveness. U.S. firms have invested heavily in technologies that make digital marketplaces safer, including advanced fraud detection, trust-and-safety systems, logistics, and AI. Competition should reward those investments. Platforms should compete by offering better products, better services, lower prices, and stronger consumer protections—not by evading those responsibilities.

APPLYING THESE PRINCIPLES TO THE PENDING BILLS

The bills before the subcommittee take different approaches to strengthening consumer protection and marketplace integrity. The following comments highlight how selected proposals align with the principles discussed in my testimony.

H.R. 6832, the Packaging and Claims Knowledge (PACK) Act of 2025

The PACK Act would establish a voluntary federal standard for environmental claims on product packaging, helping consumers better understand labels such as "recyclable," "compostable," and "reusable." Today, manufacturers often face a patchwork of state requirements, particularly as standards adopted by large states can effectively become national requirements even in the absence of a federal standard. That fragmentation can create confusion for consumers and increase compliance costs for businesses.

A voluntary federal framework would improve consistency while reducing unnecessary barriers to interstate commerce. Consumers benefit when environmental claims are clear, credible, and applied consistently across the country, and businesses benefit from operating under a common set of expectations rather than navigating conflicting state requirements. Congress should continue to look for opportunities to replace fragmented state-by-state rules with national frameworks that promote transparency, reduce compliance burdens, and preserve a truly national marketplace.

H.R. 7502, the Recycled Materials Attribution Act

The Recycled Materials Attribution Act would establish consistent federal standards for recycling and recycled content claims, replacing the current patchwork of differing state requirements. Today, manufacturers and consumers often face inconsistent definitions and labeling rules that create confusion, increase compliance costs, and discourage investment in recycling infrastructure.

A uniform national framework would improve transparency by giving consumers clearer and more consistent information about recycled content while reducing unnecessary barriers to interstate commerce. It would also provide greater regulatory certainty for manufacturers and recyclers, helping encourage investment in recycling systems and markets for recycled materials. Congress should generally favor national standards over conflicting state-by-state requirements when products move freely through interstate commerce and consumers benefit from consistent information.

H.R. 5956, the Defending Against Foreign Propaganda Act

The Defending Against Foreign Propaganda Act addresses an important transparency objective: Americans should know when the advertisements they see are funded by foreign governments or foreign entities so they can better evaluate the source and credibility of those messages. Clear disclosure requirements can strengthen consumer awareness without restricting lawful speech.

The bill could benefit from several refinements. First, it should include an appropriate knowledge standard so that advertising platforms are not held strictly liable when foreign entities conceal or misrepresent their identity. Platforms should make reasonable efforts to verify advertisers, but they should not face liability for deception they could not reasonably detect. Second, Congress should provide clearer guidance on how the disclosure requirements apply in situations where an advertiser has ties with more than one country, such as dual nationals, multinational companies, or entities with mixed ownership. Clear definitions would reduce uncertainty for platforms while ensuring that the disclosure requirement captures the foreign influence the bill is intended to address. Finally, the bill should better reflect how digital advertising works today. Its disclosure requirements assume traditional print, audio, and video formats, creating unnecessary implementation challenges for common digital formats such as silent autoplay videos, sponsored search results, interactive advertisements, and emerging immersive media. Rather than prescribing disclosures tied to specific media formats, Congress should require disclosures that are clear and conspicuous while allowing platforms flexibility to implement them in ways that best fit different advertising experiences.

H.R. 5967, the Strategic Task Force on Scam Prevention Act

The Strategic Task Force on Scam Prevention Act recognizes that combating scams requires coordination across multiple agencies and sectors. Fraud schemes increasingly span jurisdictions, technologies, and online platforms, making it important for the Federal Trade Commission, the Department of Justice, and other agencies to share information, coordinate enforcement, and identify emerging threats. The bill could be strengthened by explicitly including online counterfeiting and piracy within the task force's scope, as both increasingly serve as pathways for scams and fraud that harm American consumers. Congress should also ensure that online retailers and online marketplaces are represented among the industries consulted by the task force, as these platforms often have the earliest visibility into emerging scams and fraudulent actors.

The task force should also prioritize improving data collection, information sharing, and analytical capabilities across the federal government. Effective prevention depends on identifying patterns across complaints, marketplaces, payment systems, and other sources of information that no single agency sees on its own. Counterfeit goods, online piracy, and other forms of digital fraud should be incorporated into this broader strategy, including by establishing clearer pathways for consumers and rights holders to report suspected violations. Congress should also direct the task force to consider the use of AI and advanced data analytics to identify emerging fraud schemes, detect repeat offenders, connect related investigations across agencies, and better target enforcement resources. These capabilities can help the government move from responding to individual incidents toward proactively disrupting criminal networks.

H.R. 3875, the Transparency in Enforcement, Restricting, and Monitoring of Services (TERMS) Act

The TERMS Act advances an important principle: greater transparency helps digital markets function more effectively. Requiring online service providers to clearly disclose their acceptable use policies, explain significant enforcement actions, and publish aggregate information about how they enforce their rules can help users better understand platform practices and encourage greater consistency and accountability. Transparency also allows consumers to make more informed choices about which platforms best meet their expectations.

The bill's notice requirement would benefit from greater flexibility. Requiring platforms to provide users with seven days' advance written notice before restricting an account may be appropriate in many circumstances, but it could impede platforms from responding quickly to fraudulent accounts, hijacked accounts, counterfeit sellers, coordinated scams, and other harmful conduct that requires immediate action. Congress should preserve platforms' ability to act swiftly when necessary to protect users and the integrity of their services, while continuing to require meaningful notice and an opportunity to appeal once the immediate risk has been addressed.

H.R. 3209, the App Store Freedom Act

The App Store Freedom Act differs from many of the other bills before the subcommittee. Whereas much of today's legislation seeks to strengthen consumer protection, improve transparency, and reduce fraud, this bill could inadvertently weaken important safeguards that protect consumers from malicious software, scams, and other online harms.

Leading U.S. app stores invest heavily in app review, malware detection, fraud prevention, identity verification, and ongoing monitoring of developers. For example, Apple reported reviewing more than 9 million app submissions in 2025 and rejecting more than 2 million that failed to meet its security and safety requirements.[9] Similarly, Google reported preventing more than 1.75 million policy-violating apps from being published on Google Play and banning more than 80,000 developer accounts that attempted to distribute harmful apps.[10] These investments help protect consumers from malware, fraud, and other online threats before they reach users.

Requiring these app stores to permit sideloading and broader third-party app distribution would reduce their ability to screen for malware, fraud, and other harmful applications. Congress should carefully weigh these consumer protection risks before requiring mobile operating system providers to adopt distribution models that can weaken the security of their app ecosystems.

The BOSS and SWIFT Act of 2026

The BOSS and SWIFT Act includes several provisions that would improve transparency and strengthen consumer protections in the ticketing market. Requiring clear disclosure of the total ticket price, fees, and refund policies will help consumers make more informed purchasing decisions and encourage fairer competition among ticket sellers. The bill also appropriately addresses practices that unnecessarily restrict ticket transfers or impose artificial price floors, which can limit consumer choice and force buyers to pay additional fees.

The bill could be strengthened by recognizing that not all transfer restrictions are anti-consumer. Some event organizers (such as the Savannah Bananas) limit resale prices or impose other transfer conditions to discourage scalping, ensure tickets remain affordable, or improve the fan experience. Congress should preserve room for these pro-consumer ticketing models to compete by creating a narrow exception for reasonable transfer restrictions that demonstrably benefit consumers while maintaining meaningful transferability and avoiding vendor lock-in. This approach would protect consumers from abusive restrictions without discouraging innovative ticketing models that compete on the quality of the customer experience.

The Short-Term Rental Sex Offending Disclosure Act

The SECURED Act advances a straightforward and important consumer protection principle: consumers should have access to material safety information when making purchasing decisions. Requiring short-term rental platforms to collect information about whether a property owner is a registered sex offender and disclose that information to prospective guests would provide greater transparency and help consumers make more informed choices, particularly when traveling with children or other vulnerable family members.

Providing accurate, relevant information allows consumers to better assess risk while encouraging greater accountability in the short-term rental marketplace. ITIF generally supports measures that improve market transparency because well-informed consumers make better decisions, markets function more effectively, and platforms have stronger incentives to maintain high standards.

The Stop the Fraud Act

The Stop the Fraud Act addresses a legitimate and growing concern. As discussed throughout this testimony, Congress should evaluate online marketplaces based on the protections they provide American consumers. ITIF's research indicates that several major Chinese online marketplaces consistently fall short of the standards established by leading U.S. marketplaces, exposing consumers to greater risks from counterfeit, unsafe, and fraudulent products. Congress is therefore right to examine whether additional measures are needed to address these risks and ensure that all marketplaces serving American consumers meet comparable expectations for marketplace governance, transparency, and consumer protection.

The bill's import restriction would benefit from greater precision. As drafted, it could impose obligations on participants throughout the supply chain who may have no practical way to determine whether a particular product originated from a transaction on a covered online marketplace. For example, manufacturers, fulfillment providers, carriers, customs brokers, and other intermediaries may handle identical products destined for multiple marketplaces without knowing where a particular sale occurred. Congress should ensure that any compliance obligations fall on parties with the ability to identify and control the relevant transactions, while providing clear standards for tracing a product's marketplace of origin. Doing so would make the legislation more effective while avoiding unnecessary burdens on legitimate businesses.

CONCLUSION

Thank you again for the opportunity to testify today. Congress has an opportunity to better protect American consumers from dangerous goods, improve transparency in digital markets, and reduce fraud while preserving the benefits of online commerce. Achieving those goals requires ensuring that all online marketplaces serving American consumers—regardless of where they are headquartered—meet reasonable expectations for seller accountability, transparency, and consumer protection. Doing so will better protect consumers, reward responsible businesses that invest in marketplace integrity, and strengthen confidence in digital commerce. I appreciate the subcommittee's attention to these issues and look forward to your questions.

REFERENCES

1. Eli Clemens, "How Chinese Online Marketplaces Fuel Counterfeits," Information Technology and Innovation Foundation, August 2025, https://itif.org/publications/2025/08/20/how-chinese-online-marketplaces-fuel-counterfeits/.
2. Aditi Bharade, "Shein and Temu shoes and sandals were found with 11 to 229 times the legal limit for toxic substances, South Korean officials say," *Business Insider*, August 15, 2025, https://www.businessinsider.com/shein-temu-shoes-11-229-times-legal-limit-toxic-substances-2024-8.
3. Executive Office of the President of the United States, "Economic and Trade Agreement Between the United States of America and the People's Republic of China," January 15, 2020,

https://ustr.gov/sites/default/files/files/agreements/phase%20one%20agreement/Economic_And_Trade_Agreement_Between_The_United_States_And_China_Text.pdf.

4. Haoyu Wang et al., "Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets," September 26, 2018, https://arxiv.org/pdf/1810.07780.
5. Toy Association, "Products Purchased on Temu or Shein; Potential Safety Issues Identified," November 17, 2025, https://www.toyassociation.org/Common/Uploaded%20files/toyassociation/industryreports/temu-shein-report-summary.pdf.
6. Department of Justice, "Online Marketplace Temu to Pay $2 Million Penalty for Alleged INFORM Act Violations," September 5, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/09/online-marketplace-temu-pay-2-million-penalty-alleged-inform-act-violations.
7. Eli Clemens and Rodrigo Balbontin, "Comments to USTR Regarding the 2025 Review of Notorious Markets for Counterfeiting and Piracy," September 23, 2025, Information Technology and Innovation Foundation, https://itif.org/publications/2025/09/23/comments-ustr-regarding-2025-review-notorious-markets-counterfeiting-piracy/.
8. Office of the United States Trade Representative, "2025 Review of Notorious Markets for Counterfeiting and Piracy," https://ustr.gov/sites/default/files/files/Press/Releases/2026/2025%20Notorious%20Markets%20List%20(final).pdf.
9. Apple, "The App Store stopped over $2.2 billion in potentially fraudulent transactions in 2025," May 20, 2026, https://www.apple.com/newsroom/2026/05/the-app-store-stopped-over-2-point-2-billion-usd-in-fraudulent-transactions-in-2025/.
10. Vijaya Kaza, "Keeping Google Play & Android app ecosystems safe in 2025," Google Security, February 19, 2026, https://blog.google/security/keeping-google-play-android-app-ecosystem-safe-2025/.