ECOMMERCE INNOVATION ALLIANCE

David Carter, President & CEO
303 W. Broad Street
Richmond, Virginia 23220
david@ecomm-alliance.org
202.240.7890

October 20, 2025

The Honorable Ted Cruz, Chairman
Committee on Commerce, Science, and Transportation
United States Senate
Dirksen Senate Office Building 554
Washington, D.C. 20510

The Honorable Maria Cantwell, Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
Hart Senate Office Building 428
Washington, D.C. 20510

RE: Support for S. 2666, the Foreign Robocall Elimination Act

Dear Chairman Cruz and Ranking Member Cantwell:

On behalf of the Ecommerce Innovation Alliance (EIA), I am writing to express our strong support for S. 2666, the Foreign Robocall Elimination Act. The EIA is a nonprofit trade association representing over 15,000 ecommerce companies and dedicated to advocating for common-sense policies that strengthen the ecommerce ecosystem while protecting consumers. We commend the Committee for its focus on combating the persistent and damaging threat of illegal, foreign-originated robocalls, a problem that directly harms American consumers and the legitimate businesses that serve them. We believe S. 2666 represents a thoughtful and effective step toward restoring the integrity of our nation's communication channels.

The High Cost of Inaction: How Foreign Scams Damage the Ecommerce Sector

For the modern ecommerce industry, voice and text communications are not obsolete relics but a vital artery for essential customer interactions. From shipping notifications and fraud alerts to critical support services, these channels are indispensable. The relentless barrage of illegal calls from foreign actors, however, is systematically eroding consumer trust in the very act of answering the phone. This has created a deep and pervasive trust deficit; one 2025 study revealed that 72% of Americans do not answer calls from numbers they do not recognize.

This climate of suspicion inflicts severe collateral damage on our members, creating a cascade of operational failures that increase costs and degrade the customer experience. When a

customer ignores a call out of a rational fear of scams, it could be an urgent update about a delivery exception, leading to a returned package and a frustrated customer. It could be a fraud alert from a payment processor going unanswered, allowing a fraudulent transaction to proceed. Or it could be a customer support agent's callback being ignored, leading to a negative review and a lost customer.

The damage extends far beyond operational friction. Foreign scammers directly harm our members by hijacking their trusted brand names to defraud their own customers. Ecommerce sites are particularly attractive targets for these sophisticated brand impersonation and spoofing tactics because they are hubs of financial transactions and sensitive data. These are not random acts, but organized campaigns run by foreign-based criminal networks that use a multi-channel approach:

- **Voice and Text Impersonation (Vishing and Smishing):** Criminals use robocalls and text messages to directly target consumers, often spoofing the phone numbers of trusted brands. A 2023 survey found that 45% of brand impersonation messages mimicked "e-commerce sites and online stores". Scammers frequently impersonate major brands like Amazon with fake "suspicious charge" alerts, Apple and Microsoft with phony "security breach" warnings, and delivery carriers like FedEx or UPS with fraudulent "package delivery problem" notifications designed to harvest personal data.

- **Digital Impersonation:** Scammers create fraudulent websites, malicious search engine ads, and fake social media profiles that are nearly indistinguishable from the real thing, luring customers into revealing login credentials and financial information.

The consequences are profound. While consumers suffer immediate financial loss—with business and government impersonation scams accounting for nearly $3 billion in losses in 2024—the impersonated brand suffers lasting reputational damage. Legitimate businesses are then left to manage the costly fallout, as their customer service channels are flooded by confused and angry victims, diverting critical resources from legitimate service needs.

Finally, these foreign scams impose a significant and often overlooked operational burden. One of the most disruptive tactics is the Telephony Denial of Service (TDoS) attack, where scammers flood a business's toll-free customer service lines with thousands of automated calls, tying up communication infrastructure and preventing legitimate customers from getting through. This environment creates a vicious cycle that directly increases a key metric of ecommerce success: customer acquisition cost (CAC). As consumer distrust leads to lower answer rates for legitimate outbound calls, the return on investment for marketing campaigns

diminishes. Businesses are then forced to either increase call volumes, which carries its own legal risks, or shift to more expensive marketing channels, squeezing profitability.

S. 2666: A Measured and Effective Approach

The EIA believes S. 2666 is the right approach to this complex problem for two primary reasons.

First, it correctly targets the true culprits: international criminal organizations engaged in fraud. By focusing on *illegal foreign-originated* calls, the bill avoids the overly broad language that has characterized some state-level telemarketing laws, which often inadvertently penalize legitimate, domestic businesses communicating with their customers lawfully and with consent.

Second, the bill's greatest strength is its creation of a balanced, public-private Interagency Taskforce. This "study before you regulate" approach ensures that future policy will be driven by data and expert analysis, not reactionary impulses. We particularly commend the inclusion of dedicated seats for both marketing and non-marketing businesses. This guarantees that the taskforce will hear directly from industry stakeholders who can articulate the critical distinction between wanted, consent-based ecommerce communications and illegal scams, preventing the kind of regulatory overreach that harms lawful businesses.

The Path Forward: A Call for Common Sense Guardrails

As the Committee considers this legislation, the EIA advocates for a set of common-sense principles to guide the work of the taskforce and any subsequent policymaking:

1. **Preserve Consent-Based Communication:** The foundation of legitimate e-commerce communication is consumer consent. Any new framework must include an unambiguous safe harbor for communications made with a consumer's prior express consent.
2. **Avoid Creating New Litigation Traps:** New regulations must provide clear, actionable guidance for businesses acting in good faith. Vague or complex rules risk becoming weaponized in abusive litigation, which is a significant threat to the e-commerce industry.
3. **Promote Technological Solutions:** Policy should encourage the widespread adoption of technologies like enhanced call authentication and branded calling solutions that empower consumers and providers, rather than relying solely on punitive mandates that can be misapplied to legitimate businesses.

The Foreign Robocall Elimination Act is a constructive and well-conceived piece of legislation. It provides a sound framework for developing nuanced, practical, and technologically informed solutions that can effectively combat illegal calls without stifling the innovation and essential communications that underpin the digital economy.

The Ecommerce Innovation Alliance strongly supports S. 2666 and urges the Committee to advance it. We thank you for your leadership on this critical issue and stand ready to serve as a resource as you continue your work.

Sincerely,

G. David Carter
President and CEO
Ecommerce Innovation Alliance

Cc: Sen. Ted Budd
Sen. Peter Welch