Written Testimony of

Lori Wallach
Director, Public Citizen's Global Trade Watch

before

The Subcommittee on Consumer Protection and Commerce of the House Energy and Commerce Committee

on

"Buyer Beware: Fake and Unsafe Products"

March 4, 2020

Lori Wallach, Director
Public Citizen's Global Trade Watch
215 Pennsylvania Ave. SE
Washington, D.C. 20003
lwallach@citizen.org
202-546-4996

Madam Chairwoman and Members of the Committee, thank you for the opportunity to testify today on the serious threats posed to American consumers by a tsunami of unsafe products facilitated by e-commerce sales. I am Lori Wallach, director of Public Citizen's Global Trade Watch. Public Citizen is a national public interest organization with more than 500,000 members and supporters. For more than 45 years, we have advocated with some considerable success for consumer protections and more generally for government and corporate accountability. The Committee is performing a vital service by elevating public attention to these threats to which numerous Americans are being exposed, exploring the gaps in current policy and practice created by the growing flood of largely unregulated online commerce and considering remedies to improve consumer safety.

When many people think of fake products, they imagine knockoff Gucci bags or Rolexes and street vendors or flea markets selling counterfeit goods that violate brand-name trademarks. But increasingly, and to a great extent *because of* the exponential growth of e-commerce as a means by which Americans buy products, consumers are being *widely* exposed to serious consumer health and safety risks by "fake" products. Fake and unsafe products produced anywhere in the world gain millions of potential customers with sales and delivery made easy and quick and listing on well-branded e-commerce platforms providing an air of legitimacy and false sense of safety.

Many major e-commerce retailers' focus on expanding sales has come to the detriment of consumer health and safety. The platforms claim that they are not sellers of the goods, despite providing marketing and curating what consumers view on their platforms, providing consumers access to the goods, collecting consumers' payments and delivering the goods to purchasers. Claiming not be the sellers, the platforms assert that they, thus, are not responsible for health and safety problems or false representations related to the products nor legally liability when consumers are injured. This dynamic creates market signals that reward exposing consumers to untenable risks. It also is fundamentally unfair to brick and mortar retailers and the producers of legitimate and safe goods, who have legal responsibilities that incentivize them to consider consumer safety and punish them for the sales of fake and dangerous goods that occur numerous times every minute on e-commerce platforms. Moreover, the e-commerce platforms shift to legitimate producers the financial responsibility of trying to police against dangerous knockoffs of their products, with legitimate producers forced to play an endless and often futile game of whack-a-mole as they try to catch counterfeit versions of their goods being offered on major online sales platforms and get the platforms to take down the listings, which are then replaced by a new listing for the same knockoff within days.

Many consumers remain unaware of the risks, or even that numerous products that they have purchased online on well-known e-commerce sites are not what the consumer assumes that they are and may well be dangerous. And many of the platforms make it very difficult for even the most conscientious consumer to decipher exactly what product they are ordering and from where it actually will be sourced. As has been made evident by the many recent press exposés about consumers killed or injured by goods sold online, most online buyers assume that when they make purchases from a well-known e-commerce platform, goods come from the firm with the related assumption that the online retailer is responsible for ensuring the good is safe.

The U.S. government agencies responsible for ensuring product safety are entirely overwhelmed by the volume of online sales, in most instances have not brought operations up to date with the reality that a growing share of products are sold online and are produced outside the United States, and in some instances do not have the statutory or regulatory authority to ensure consumer health and safety related to online commerce. And some recent U.S. policy changes have

increased the risk of consumers being exposed to unsafe goods bought online. Online retailers and express shippers celebrated enactment of the 2015 Trade Facilitation and Trade Enforcement Act (TFTEA), which raised to $800 from $200 the value of imported goods subject to a "de minimis" waiver. Goods with a value below the de minimis, imported by one person on one day, can be admitted free of duty and taxes under §321 of the Tariff Act of 1930. This has created a major new safety threat, as these goods are not subject to the same formal customs procedures and rigorous data requirements as higher-value shipments entering the United States.[1] Absence of an Harmonized Tariff Schedule code or standardized product description such as a Standard Industrial Classification (CIS) code and producer identification was not risky in the context of $200 of goods returning with an overseas traveler. But raising the de minimis to $800 means enormous volumes of e-commerce-purchased goods enter the United States in a way that makes it virtually impossible for government agencies to identify goods – such as airbags, products for babies, scooters, medical equipment and more – that pose high risks to consumer health and safety. Currently, approximately 1.8 million shipments a day are released pursuant to Section 321.[2] The majority of these Section 321 shipments are arriving by air and truck. The Consumer Product Safety Commission (CPSC) estimates that in 2023, 55 million *de minimis* e-commerce shipments that would fall under Consumer Product Safety Commission's jurisdiction will enter the country – *not* including packages arriving by mail.[3] Without having the data to identify high risk goods, the CPSC reports that it inspects almost no de minimis shipments. Some countries are considering lowering de minimis levels to capture the flood of online retail shipments skirting inspections, and with very few exceptions other nations' de minimis levels now are lower than $200.[4] Further, Customs considers each online consumer to be the importer, not the online retailer. Customs requires advanced, detailed information for ocean shipping containers bringing imported goods for sale in brick and mortar stores, and these goods are subject to inspections and, if applicable, tariffs and taxes. But containers of goods sold on major online platforms, if picked and packed at overseas fulfillment centers and addressed to consumers, are not. Nor are a million-plus air shipments bringing in e-commerce purchases just from China every day. Now, operations in Mexico and Canada are receiving ocean container-shipped goods in bulk, for satisfaction of e-commerce orders at a much lower cost than air freight. These goods are considered to be in transit to the United States, and thus outside customs requirements in those countries. They are separated into packages for delivery to U.S. consumers and, being under $800 per package, are trucked over the border to U.S. post offices and express shippers, skirting U.S. Customs and inspection.[5]

The Scope of the Problem

The problem of fake and/or unsafe products purchased online has intensified to staggering levels as e-commerce has rapidly expanded. In February 2019, the Commerce Department's Retail Sales Report showed the total market share of "non-store," or online U.S. retail sales was higher than general

[1] 19 CFR § 10.151 and 19 CFR part 143, Subpart C
[2] 84 Fed. Reg. 354056, Department of Homeland Security: Section 321 Data Pilot General Notice. (July 23, 2019). Available at https://www.govinfo.gov/app/details/FR-2019-07-23/context
[3] CPSC e-Commerce Assessment Report, United States Consumer Product Safety Commission, Office of Import Surveillance, Nov. 2019 at page 9. Available at: https://www.cpsc.gov/s3fs-public/CPSC%20e-Commerce%20Assessment%20Report.pdf?B.5pu7oFYPRJsokNjHygmRyZVo0tpPmE See footnote 9: "Note that the volume estimates in this report do not account for e-Commerce that arrives via international mail. CBP estimates that 475 million total mail shipments arrived in the United States in 2018. Available data, however, did not allow EXIS to estimate the number of international mail e-Commerce shipments arriving under its jurisdiction."
[4] See https://www.zhenhub.com/2018/05/15/customs-duty-de-minimis-values-by-country/ for de minimis levels by country.
[5] Lydia DePillis, "How Trump's Tariffs Are Creating Jobs — for Canadians," Pro Publica, Oct. 9, 2019, 5 a.m. EDT https://www.propublica.org/article/how-trump-tariffs-are-creating-jobs-for-canadians

merchandise sales for the first time.[6] This trend has continued with the February 2020 Census data showing a continuing trajectory of faster growth in e-commerce than in overall retail generally.[7] The White House Office of Trade and Manufacturing Policy reports that more than one million de minimis packages enter the United States just from China via air shipments daily.[8] In a 2017 special enforcement action, Customs and Border Protection officers randomly examined more than half of the express-mail packages arriving daily from Hong Kong and mainland China over a five-day period – and seized 43 percent of them as noncompliant imports, including counterfeit pharmaceuticals (along with controlled substances, including fentanyl).[9]

The CPSC Office of Import Surveillance (EXIS) published an "e-Commerce Assessment Report" in November 2019 that documented the steady growth of the value and the volume of e-commerce shipments under the CPSC's jurisdiction entering the United States. Noting that "the quadrupling of the *de minimis* threshold value for imports…has increased the volume of small packages entering the United States"[10] the agency focused its assessment on de minimis shipments.

The value of e-commerce shipments CPSC regulates is estimated to reach $415 billion by 2023, which will represent almost 38 percent of the total value of imports under the agency's jurisdiction.[11] Notably, because of the lack of data, these figures exclude e-commerce shipments delivered by international mail, meaning the figures represent an undercount.[12] The countable $886 billion in shipments under CPSC jurisdiction in 2018 is projected to grow to more than $1.1 trillion by 2023. Currently about 30 percent ($260 billion) is e-commerce purchases. This number is projected to grow to 38 percent, or $415 billion, by 2023, excluding goods delivered by international mail. The growth rate for goods under CPSC jurisdiction is significantly higher than for U.S. imports as a whole.

The CPSC assessment estimates that 65 million imported shipments under CPSC's jurisdiction entered the United States in 2018, with an estimated 36 million of them being e-commerce purchases. E-commerce goods under CPSC jurisdiction are expected to rise to 60 million by 2023, meaning such goods will be about 57 percent of the total volume of imports under CPSC's jurisdiction.[13] Again, available data did not allow a determination of the number of international mail e-commerce shipments arriving under CPSC jurisdiction; however, U.S. Customs and Border Protection (CBP) estimates that 475 million total international mail shipments arrived in the United States in 2018.

---

[6] "Online shopping overtakes a major part of retail for the first time ever," Kate Rooney, CNBC, Apr. 2, 2019 .
[7] Quarterly Retail E-Commerce Sales, 4th quarter 2019, U.S. Census Department, Feb. 19, 2020. Available at https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf
[8] On-the-record-press-call, Assistant to the President for Trade and Manufacturing Policy Peter Navarro on an Executive Order Ensuring Safe and Lawful E-Commerce, Jan. 31, 2020. Available at https://publicpool.kinja.com/subject-on-the-record-press-call-on-an-executive-order-1841396650?utm_medium=sharefromsite&utm_source=_twitter
[9] Peter Navarro, "When you buy online via Alibaba, Amazon or eBay, chances are high you'll end up with a counterfeit," Wall Street Journal oped, Apr. 2, 2019. Available at https://www.wsj.com/articles/trump-has-a-plan-to-stop-fake-goods-11554246679
[10] CPSC e-Commerce Assessment Report, United States Consumer Product Safety Commission, Office of Import Surveillance, Nov. 2019 at page 18, see figure 16. Available at: https://www.cpsc.gov/s3fs-public/CPSC%20e-Commerce%20Assessment%20Report.pdf?B.5pu7oFYPRJsokNjHygmRyZVo0tpPmE
[11] Id. at page 15. Per footnote 2, figures were calculated based on the number of House Bills of Lading filed with Customs and Border Protection (CBP) for shipments at or under $800 plus the number of filed Entries for shipments over $800.
[12] See Id. at footnote 9: "Note that the volume estimates in this report do not account for e-Commerce that arrives via international mail. CBP estimates that 475 million total mail shipments arrived in the United States in 2018. Available data, however, did not allow EXIS to estimate the number of international mail e-Commerce shipments arriving under its jurisdiction."
[13] Id. at page 1.

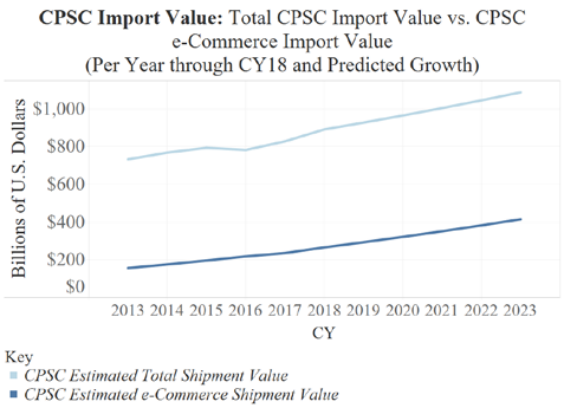


Figure 1: Import Value under CPSC's Jurisdiction

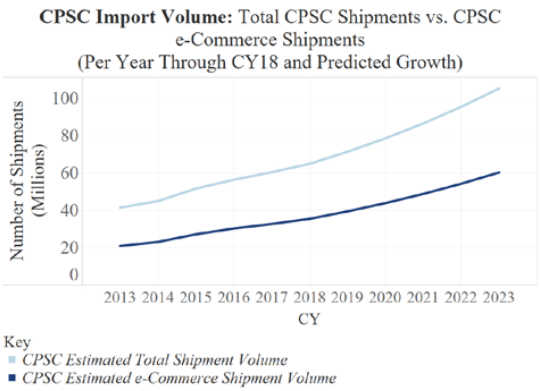


Figure 2: Import Volume under CPSC's Jurisdiction

The CPSC "E-Commerce Assessment Report" notes: "The rapid rise of e-Commerce introduces new challenges to EXIS, which is responsible for identifying and examining high-risk imported products. CPSC's ability to stop unsafe shipments in the e-Commerce environment is limited, in part, due to the sheer volume of low-value shipments, as well as the locations where they arrive." The mismatch between CPSC resources and staffing and the growing volume of and means of entry of e-commerce shipments is discussed further, below.

There is little disagreement that e-commerce is increasing the sale of fake goods. A 2018 U.S. Government Accountability Office (GAO) report concluded that that e-commerce has contributed to a shift in the sale of counterfeit goods in the United States, with consumers increasingly purchasing goods online and counterfeiters producing a wider variety of goods that may be sold on websites alongside authentic products.[14] It is worth nothing that these challenges are not unique to the United States. A 2018 Organization for Economic Cooperation and Development (OECD) report, *Governance Frameworks to Counter Illicit Trade*, noted: "E-commerce platforms represent ideal storefronts for counterfeits… and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers."[15] A 2016 OECD report identified a trend towards small shipments for sellers of fake goods, noting that a review of global customs seizure data found that one-third was single items.[16] The same data review identified China as the source of almost two-thirds of counterfeit goods globally. Hong Kong was the second largest, and Turkey, Singapore and Thailand were the next most frequent, but in much smaller volumes.

Of the contraband products seized in 2018 by U.S. Customs and Border Protection (CBP), an astonishing 16 percent posed direct and obvious threats to health and safety.[17] Recently, CBP has conducted several intensive inspection blitzes of e-commerce de minimis shipments at seven of CBP's

[14] U.S. Government Accountability Office Report to the Chairman, Committee on Finance, U.S. Senate: *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, GAO-18-216, Government Accountability Office, Jan. 2018 at page 18. Available at https://www.gao.gov/assets/690/689713.pdf

[15] OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, at page 84-85. Available at https://doi.org/10.1787/9789264291652-en

[16] Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing - ECD/EUIPO, 2016 at page 51 and 56. Available at https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147

[17] Department of Homeland Security, U.S. Customs and Border Protection, "Intellectual Property Rights: Fiscal Year 2018 Seizure Statistics," Aug. 2019. https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf

international mail facilities and four express consignment hubs. Among the items found were weapon modifications, silencers and other gun parts; counterfeit contact lenses, auto parts, bike helmets, infant formula, and sports equipment made with faulty parts; and banned drugs, pill presses, steroids and addictive painkillers like Tramadol.[18]

The CPSC, OECD and U.S. Government Accountability Office (GAO) reports, as well as a January 2020 report by the Department of Homeland Security, "Combating Trafficking in Counterfeit and Pirated Goods,"[19] all note that while frequently seized counterfeit goods include clothing, watches, perfumes and leather goods, products that pose significant consumer health and safety risks are also among top fake goods. This includes toys, machinery and spare parts, products for babies and children from car seats to cribs, pharmaceuticals, cosmetics and more. In December 2015, CBP seized 1,378 hover boards with counterfeit batteries, which can cause fires resulting in injury or death.[20] An investigation of counterfeit iPhone adapters conducted by Underwriters Laboratory found a 99 percent failure rate in 400 counterfeit adapters tested for safety, fire and shock hazards, and found that 12 of the adapters posed a risk of lethal electrocution to the user.[21] The Department of Justice prosecuted importers bringing in fake, unsafe airbags,[22] which along with other counterfeit automotive parts like brake pads, wheels and seat belts can have catastrophic consequences for drivers, as well as for their passengers and others on the road.

Recent CNN and Wall Street Journal exposés, "Fake and Dangerous Kids Products Are Turning Up for Sale on Amazon" and "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," found that children's toys – some laced with deadly metals like cadmium and lead, others with powerful magnetic pieces that tear children's' intestines when swallowed as well as unsafe baby strollers, cribs and sleepers – represent another area in which counterfeiters have taken advantage of e-commerce business models that provide limited to no accountability for sellers.[23] Fake and unsafe imported bicycle and motorcycle helmets have also caused severe injury and death to U.S. consumers who purchased these goods online, as noted in the recent Wall Street Journal exposé which found 44 models that failed federal safety tests in 2018.[24]

---

[18] Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States, Department of Homeland Security, Jan. 24, 2020 at page 9, citing Department of Homeland Security, U.S. Customs and Border Protection, Operation Mega Flex I, II and III Summaries, 2019. Available at https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

[19] Id.

[20] U.S. Customs and Border Protection, CBP at JFK seizes Counterfeit Hoverboards with Potentially Dangerous Batteries, press release, Feb. 19, 2016. Available at https://www.cbp.gov/newsroom/local-media-release/cbp-jfk-seizes-counterfeit-hoverboards-potentially-dangerous-batteries

[21] Underwriters Laboratory (UL), "Counterfeit iPhone Adapters", available at: https://legacy-uploads.ul.com/wp-content/uploads/sites/40/2016/09/10314-CounterfeitiPhone-WP-HighRes_FINAL.pdf.

[22] Department of Justice, U.S. Attorney's Office, Western District of New York, "Two Men Charged with Importing and Selling Counterfeit Airbags," 24 Oct. 2016. https://www.justice.gov/usao-wdny/pr/two-men-charged-importing-and-selling-counterfeit-airbags; Department of Justice, U.S. Attorney's Office, Western District of New York, "Cheektowaga Man Sentenced for Buying and Selling Counterfeit Airbags," May 9, 2019.

[23] Pamela Boykoff and Clare Sebastian, "Fake and Dangerous Kids Products Are Turning Up for Sale on Amazon", CNN, Dec. 23, 2019. Available at https://www.cnn.com/2019/12/20/tech/amazon-fake-kids-products/index.html ; Alexandra Berzon, Shane Shifflett and Justin Scheck, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," Wall Street Journal, Aug. 23, 2019 Available at https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990

[24] Alexandra Berzon, Shane Shifflett and Justin Scheck, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," Wall Street Journal, Aug. 23, 2019 Available at

The Wall Street Journal conducted a major investigation that found 4,152 items for sale on Amazon's website, 46 percent of which were listed as shipping from Amazon warehouses, that were deemed unsafe or banned by federal agencies or that were deceptively labeled. This included at least 2,000 listings for toys and medications that lacked warnings about health risks to children. Among the items found were 157 products that Amazon had said it banned, including 80 listings for infant sleeping mats that the Food and Drug Administration (FDA) has warned can cause suffocation. Also found were more than 1,000 electronics products falsely labeled as Underwriters Laboratory-approved and 16 products falsely listed as FDA-approved including eyelash-growth serum that never undertook the drug-approval process. Some 77 listings contained numerous magnetic balls or cubes that federal regulators have called a substantial product hazard. The Wall Street Journal had tested by a product safety laboratory10 children's products purchased on Amazon, including those it reported were promoted as "Amazon's Choice." Four failed tests based on federal safety standards, including one with lead levels that exceeded federal limits. Amazon took down many items that Wall Street Journal investigators flagged. But scores of these goods reappeared again later and were only removed when the Wall Street Journal again contacted Amazon.

While the sale of unsafe products is a problem across e-commerce platforms, the attention paid to Amazon reflects the reality that it is the world's largest e-commerce platform, and its dominance is growing. Amazon now controls 37.7 percent of U.S. e-commerce sales, and that share is expected to grow, according to an assessment from data company eMarketer.[25] A February 2020 Bank of America investor memorandum estimates Amazon currently has about 44 percent of U.S. e-commerce market share, up from 40 percent in 2018. Walmart is a distant second at just 7 percent, followed by eBay at 5 percent and Target at just 2 percent.[26] The Bank of America memo spotlighted that market share trends underscore Amazon's dominance, noting that Amazon generated $79.8 billion in U.S. gross merchandise volume in the fourth quarter of 2019, up 19 percent from a year ago while eBay generated $8.9 billion, down 8.3 percent.

Who Is Selling What Online: Special Concerns Related to Third-Party Sellers

A feature of most major online platforms is the offering of goods provided by third-party sellers. One basis for the platforms' claims that they are not sellers is that a portion of the sales on their platforms is being facilitated by them for third parties. Amazon's 2018 Annual Report to Shareholders noted that its third-party sales were increasing most dramatically. (The firm's 2019 annual report is not yet out.) Third-party sales constituted 58 percent of Amazon's gross merchandise sales in 2018, compared with 30 percent a decade ago and three percent in 1999:

> "Something strange and remarkable has happened over the last 20 years. Take a look at these numbers: 1999 3%, 2000 3%, 2001 6%, 2002 17%, 2003 22%, 2004 25%, 2005 28%, 2006 28%, 2007 29%, 2008 30%, 2009 31%, 2010 34%, 2011 38%, 2012 42%, 2013 46%, 2014 49%, 2015 51% 2016 54%, 2017 56%, 2018 58% The percentages represent the share of physical gross merchandise sales sold on Amazon by independent third-party sellers – mostly small- and medium-sized businesses – as opposed to Amazon retail's own first party sales. Third-party sales

https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990

[25] Andrew Lipsman, US Ecommerce 2019: Mobile and Social Commerce Fuel Ongoing Ecommerce Channel Shift, eMarketer Report, Jun. 27, 2019. Available at https://www.emarketer.com/content/us-ecommerce-2019

[26] Wayne Duggan "Latest E-Commerce Market Share Numbers Highlight Amazon's Dominance," Benzinga, Feb. 4, 2020. Available at https://www.benzinga.com/analyst-ratings/analyst-color/20/02/15247764/latest-e-commerce-market-share-numbers-highlight-amazons-dominance

have grown from 3% of the total to 58%. To put it bluntly: Third-party sellers are kicking our first party butt. Badly. And it's a high bar too because our first-party business has grown dramatically over that period, from $1.6 billion in 1999 to $117 billion this past year. The compound annual growth rate for our first-party business in that time period is 25%. But in that same time, third-party sales have grown from $0.1 billion to $160 billion – a compound annual growth rate of 52%. To provide an external benchmark, eBay's gross merchandise sales in that period have grown at a compound rate of 20%, from $2.8 billion to $95 billion."[27]

The CBP report "Combating Trafficking in Counterfeit and Pirated Goods" also focused on third-party marketplaces as an aspect of e-commerce of elevated concern with respect to the sale of fake and unsafe goods:

> "Third-party online marketplaces can quickly and easily establish attractive "store-fronts" to compete with legitimate businesses. On some platforms, little identifying information is necessary to begin selling. A counterfeiter seeking to distribute fake products will typically set up one or more accounts on online third-party marketplaces. The ability to rapidly proliferate third-party online marketplaces greatly complicates enforcement efforts, especially for intellectual property rights holders. Rapid proliferation also allows counterfeiters to hop from one profile to the next even if the original site is taken down or blocked. On these sites, online counterfeiters can misrepresent products by posting pictures of authentic goods while simultaneously selling and shipping counterfeit versions. Counterfeiters have taken full advantage of the aura of authenticity and trust that online platforms provide. While e-commerce has supported the launch of thousands of legitimate businesses, their models have also enabled counterfeiters to easily establish attractive "store-fronts" to compete with legitimate businesses. Platforms use their third-party marketplace functions to leverage "two-sided" network effects to increase profitability for the platform by adding both more sellers and more buyers. Because sellers benefit with each additional buyer using the platform (more consumers to sell to), and buyers are more likely to join/use the platform with each additional seller (more sellers to buy from), there can be diminished internal resistance to adding lower quality sellers."[28]

The design of some platforms makes it difficult for consumers to discern who is actually selling a good. For instance, the Wall Street Journal reported that third-party items it examined were listed as Amazon Prime eligible and sold through the Fulfillment by Amazon program, which generally ships items from Amazon warehouses in Amazon-branded boxes. The actual seller's name appeared only in small print on the listing page.

In addition, the incentives on platforms to continually expand offerings undermine careful scrutiny and approval of third parties, and the ability to police what is being offered for sale. Amazon's third-party seller information and requirements includes notice that all sellers "must comply with all laws and regulations and with Amazon's policies. The sale of illegal, unsafe, or other restricted products listed on these pages, including products available only by prescription, is strictly prohibited."[29] Yet repeated

---

[27] Amazon, 2018 Annual Report to our Shareholders. Available at https://ir.aboutamazon.com/static-files/0f9e36b1-7e1e-4b52-be17-145dc9d8b5ec

[28] Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States, Department of Homeland Security, Jan. 24, 2020 at page 11. Available at https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf

[29] See https://sellercentral.amazon.com/gp/help/external/help-page.html?itemID=521&language=en_US&ref=efph_521_bred_200164330 "Customers trust that they can always buy with confidence on Amazon. Products offered for sale on Amazon must comply with all laws and regulations and with Amazon's

investigations, including in the past year by CNN and the Wall Street Journal, revealed that third-party sellers are not meeting these rules. And, until notified of violations, Amazon has not taken action to enforce the rules, and even after doing so violating goods have often reappeared.

The lack of scrutiny may be related to e-commerce platforms' claims to not being sellers subject to product liability, meaning the care brick and mortar stores give to avoid liability is absent. With respect to policing of third-party offerings, over the past weekend, numerous items listed on Amazon's seller central prohibited list[30] appeared for sale on the platform. This included roadside flares, toy crossbows

---

policies. The sale of illegal, unsafe, or other restricted products listed on these pages, including products available only by prescription, is strictly prohibited. If you supply goods on Amazon, you should carefully review the Restricted Products Help pages listed below before listing a product. The examples provided in these Help pages are not all-inclusive and are provided solely as an informational guide. We encourage you to consult with your legal counsel if you have questions about the laws and regulations concerning your products. Even where a product is listed as an "Example of Permitted Listings," all products and listings must also comply with applicable laws. In addition, any links provided are for informational purposes only, and Amazon does not warrant the accuracy of any information provided in these links. If you supply a product in violation of the law or any of Amazon's policies, including those listed on the Restricted Products pages, we will take corrective actions, as appropriate, including but not limited to immediately suspending or terminating selling privileges, destroying inventory in our fulfillment centers without reimbursement, returning inventory, terminating the business relationship, and permanent withholding of payments. The sale of illegal or unsafe products can also lead to legal action, including civil and criminal penalties. We are constantly innovating on behalf of our customers and working with regulators, third party experts, vendors, and sellers to improve the ways we detect and prevent illegal and unsafe products from reaching our marketplace. Amazon encourages you to report listings that violate Amazon's policies or applicable law by contacting us. We will investigate each report thoroughly and take appropriate action."

[30] See Amazon Seller Central's Hazardous and Dangerous Items, Examples of prohibited listings. Available at: https://sellercentral.amazon.com/gp/help/external/help.html?itemID=200164570&language=en_US&ref=efph_200164570_cont_200164330

- Products containing Bisphenol A (BPA)
  - Items containing Carbon Tetrachloride, such as: Fire extinguishers, Refrigerants, Cleaning agents
- Any chemical substance or compound that is intended for commercial, industrial, or professional use only and is not available for general consumer purchase
  - Explosives, such as: Black powder, Caps for toy guns, Explosive fuses, Exploding rifle targets, Fireworks, such as: Firecrackers, Firework kits, Aerial bombs, Bottle rockets, Party poppers, Roman candles, Smoke bombs, Snap caps, Sparklers, Flares, such as projectile and road flares, Flash paper, Gasoline
- Sky lanterns or floating lanterns
- Bacteria cultures or other products containing E coli or Escherichia coli
- Hydrofluoric acid
- Inflatable Neck Floats for children
- Information on how to make explosive devices, such as bombs
- Kite strings that are intended for kite fighting
- Military-style gas masks and their filters
- Nitric acid
- Products containing red phosphorous
- Products containing thermite
- Products containing tritium that do not comply with the regulations of the United States Nuclear Regulatory Commission
- Products that do not comply with the Safe Drinking Water Act
- Used oil, such as cooking oil or motor oil
- Water walking balls
- Products contaminated by radiation
- Liquid mercury and products containing mercury, such as:
  - Automotive switches, relays, and diostats, Batteries, with the exception of alkaline-manganese button cell batteries containing up to 25 mg of mercury, Manometers, sphygmomanometers, and other medical devices containing mercury, Mercury-added consumer novelty products such as toys, games, cards, jewelry, apparel, and footwear, Thermometers, Thermostats, Wheel weights
- Products containing cyanide
- Individual magnets or magnet sets that are small enough to fit inside a cylinder that is 1.25 inches (31.7 mm) in diameter and 2.25 inches (57.1 mm) long (For example: "small parts cylinder" or "choking tube") and have a flux index greater than 50 kg²mm² (50 kg2mm2) are prohibited from sale. Specifically, this includes individual magnets and magnet sets that are marketed or commonly used as a manipulative or construction items for entertainment, such as puzzle working, sculpture building, mental stimulation, or stress relief. Additionally, the following magnet set brands are specifically prohibited for sale: Buckyballs, Buck balls, Buckybars, ,Bucky Bigs
  - Buckycubes, CyberCube, Dynocube, Hurry Harris balls, Magnicube (also called 'Mag Cube'), Neocubes, Neocubix, Nanodots, Neo spheres, Puzzle Spheres (ONLY if they are magnets or magnetic), Zen magnets set.
- Prohibited ozone-depleting substances (ODS), such as:

shooting sharp objects, small magnet building sets, floating paper lamps, military style gas masks, and caps for toy guns.

A perusal of Amazon's rules for setting as a third party seller reinforces the Wall Street Journal's conclusion that "Amazon openly encourages anyone to sign up and start selling right away unless something in their registration or initial posting triggers the automated tools to flag them for more vetting." [31] Most categories of goods require no preapproval of products.[32] For instance, no approvals are required to sell baby products, health and personal care, outdoor Gear including for cycling, and action sports, power tools, electrical or plumbing. While several categories of goods with health implications, such as food, automotive and power sports require approvals, the approval requirement for other goods appear to focus on intellectual property enforcement, not safety concerns including for watches; video, DVD and blu-ray; and sports collectibles. Baby products are listed as possibly requiring approvals for holiday selling, with qualifications focused on being able to deliver ordered goods on time.

After the Wall Street Journal investigative report was published, on August 23, 2019 Amazon published a blog detailing its efforts to ensure goods on its third-party marketplace are safe, which noted that the firm invested more than $400 million in 2018 to "ensure products offered are safe, compliant, and authentic."[33] Interestingly, on August 22, it issued a news release announcing that it had launched 150 new tools to help sellers grow their businesses on the third-party market place and that it intended to invest $15 billion to "empower" such sellers.[34]

Challenges Faced by U.S. Government Agencies Responsible for Ensuring Safety

Given the volume of low-value imports associated with online sales, absent changes to e-commerce platforms' practices, there is no way for government safety agencies to inspect and seize consumers' way to safety. However, even if online sales platforms were subject to new safety regulation and made legally responsible as sellers, improvements would be required in government oversight and inspection. With respect to matters within this subcommittee's jurisdiction, the November 2019 CPSC e-Commerce Assessment Report provides a thorough overview of challenges face by that agency in trying to pursue its mandate in the e-commerce context and possible means to address them. This section of my written testimony summarizes the findings of the report, which in sum are:

- Appliances prohibited by EPA because they contain certain ozone-depleting refrigerants
- Class I and Class II ODS prohibited by EPA, as well as blends of prohibited ODS, and products containing prohibited ODS
- Substitutes for Class I or Class II ODS that are not reviewed and approved by EPA in accordance with the Significant New Alternative Policy Program, as well as substitute refrigerants that are subject to sales restrictions under EPA regulations and are not eligible for any exemption
- Vehicle airbags and airbag covers
- Toy crossbows that have the capability of shooting small, sharp projectiles (e.g., toothpicks, pins)

[31] Alexandra Berzon, Shane Shifflett and Justin Scheck, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," Wall Street Journal, Aug. 23, 2019 Available at https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990

[32] See https://services.amazon.com/services/soa-approval-category.html

[33] See https://blog.aboutamazon.com/company-news/product-safety-and-compliance-in-our-store

[34] https://press.aboutamazon.com/news-releases/news-release-details/amazon-announces-150-new-tools-and-services-have-launched-2019

"Although the anticipated growth of this category alone poses operational challenges, the differences in importation methods, data requirements, and other issues introduce factors that EXIS [CPSC's Office of Import Surveillance] was neither designed for, nor does it have the resources to address."[35]

However, because many of the CPSC's challenges relate to the ways in which other agencies, especially CBP, now handle e-commerce de minimis shipments, it is useful to first review the current situation. Currently, CBP requires the electronic transmission of certain information relating to commercial cargo prior to its arrival in the United States by any mode of commercial transportation.[36] This "Entry" data allows for the identification of high-risk cargo.[37] Although the required data differ for each mode of transportation and shipment type, as a general matter CBP must be informed of the shipper's name and address, the consignee name and address, a description of the cargo, including the cargo's quantity and weight, and information regarding the cargo's trip, such as trip/flight number, carrier code, point of arrival and point of origin. The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) authorizes CBP to promulgate regulations to require the electronic transmission of additional data elements for improved high-risk targeting for cargo arriving by vessel.[38] Generally required are the names and addresses of the seller, buyer, and manufacturer or supplier, the consignee identifying number, the ship to party (the first deliver-to party scheduled to receive the goods after the goods have been released from Customs custody), country of origin, Harmonized Tariff Schedule of the United States (HTS) number, container stuffing location, and the name and address of the consolidator.[39] CBP uses the advance electronic data to identify and target high-risk shipments of commercial cargo arriving in the United States and to inform other agencies such as CPSC, the Food and Drug Administration, and others so that their inspectors who are "collocated" in ports with the highest volumes of consumer products can engage.

In contrast, most e-commerce imports are subject to the Section 321 de minimis rules and are not subject to such "Entry" information requirements. This is a serious problem for protecting consumer health and safety because CPSC has developed a targeting system, called RAM or "Risk Assessment Methodology," that uses Entry data received from CBP. The CBP data is combined with CPSC data to risk-score shipments under CPSC's jurisdiction. (For instance, CPSC's Office of Import Surveillance has a list of HTS codes for products considered higher-risk.) This allows CPSC to target goods with known safety risks, such as holiday lights, cell phone wall chargers, lithium-ion batteries used in hoverboards, numerous toys and more.

CRITICAL DATA MISSING: Thus, a first problem is that currently, CPSC's Office of Import Surveillance cannot risk-assess and target products with a high risk for consumer health and safety threats shipped under the de minimis threshold because the limited data required for such shipments lack a Harmonized Tariff Schedule code or standardized product description, as well as identifiers for the importer and foreign manufacturer. Even as a large number of low-value shipments enter the country daily, CPSC's Office of Import Surveillance cannot risk-assess and target them and could not unless it could, at a minimum, obtain real-time access to manifest data and the ability to risk-assess such data. (A manifest is required of all shipments regardless of value, but it does not provide much data, and in the context of some e-commerce shipments may be only a paper form.) CBP has targeting

[35] CPSC e-Commerce Assessment Report, United States Consumer Product Safety Commission, Office of Import Surveillance, November 2019 at page 3. Available at: https://www.cpsc.gov/s3fs-public/CPSC%20e-Commerce%20Assessment%20Report.pdf?B.5pu7oFYPRJsokNjHygmRyZVo0tpPmE
[36] Public Law 107–210, 116 Stat. 933 (Aug. 6, 2002) (codified at 19 U.S.C. 1415).
[37] See 68 FR 68140 (Dec. 5, 2003); 19 CFR 4.7 (vessel), 122.48a (air), 123.91 (rail), and 123.92 (truck).
[38] Public Law 109–347, 120 Stat. 1884 (Oct. 13, 2006) (codified at 6 U.S.C. 901).
[39] See 19 CFR part 149 (the Importer Security Filing or ISF regulations).

systems that include manifest data, but in its e-Commerce Assessment report, the CPSC reported it is unclear if CPSC will be able to use the systems effectively with current staffing and operating constraints. Furthermore, due to the lack of detail in manifest data, namely the absence of an HTS code, will make it difficult to determine whether a product falls under CPSC's jurisdiction even if access to manifest data or manifest-based targeting systems is acquired. Although manifests must include a product description, it is a non-standardized field into which ambiguous or inaccurate information can be written. Finally, given the fact that there is only a short time lag between availability of data and possible clearing of a good, it could be challenging for CPSC to develop an accurate targeting methodology based on the manifest data alone.

Finally, the assessment report notes that the Consumer Product Safety Improvement Act (CPSIA) requires domestic manufacturers or importers to certify compliance of their product via a Children's Product Certificate (CPC) or a General Certificate of Conformity (GCC) and that these documents must be made available to CPSC and CBP as soon as the product or shipment is available for inspection. (A CPC certifies that a children's product complies with applicable safety rules based on test results from a CPSC-accepted third-party lab. A GCC certifies that a non-children's (general use) product complies with all applicable consumer safety rules.) How this requirement would apply in an e-commerce de minimis shipment context is unclear.

The lack of de minimis data even as the volume and thus combined value of de minimis shipments has exploded since the de minimis level was raised to $800 is a problem for numerous agencies, including CBP. In the spring of 2019, CBP initiated a voluntary Section 321 Data Pilot to test the feasibility of obtaining advance information via electronic transmission from regulated (e.g., shippers) and non-regulated entities, such as online marketplaces, as well as requiring additional advance data elements.[40] While the Federal Register notice does not specify how this would relate to "Partner Government Agencies" (CPSC, FSA, FSIS, and others who collocate with CBP at ports of entry), the CPSC e-Commerce Assessment Report notes that part of the pilot would involve allowing certain health and safety agencies to receive via a PGA Message Set additional data elements on de minimis shipments. (A PGA Message Set is a data set and the means through which an importer can satisfy a government agency's specific reporting requirements in CBP systems.) However, the CPSC e-Commerce Assessment report notes that because CPSC does not have additional data reporting requirements, CPSC's Office of Import Surveillance anticipates that it will benefit little from the test and will continue to experience the data and targeting challenges described above. As well, CPSC and many other PGA agencies CPSC surveyed in its e-Commerce Assessment report anticipate challenges in processing additional data from CBP's Entry Type 86 pilot program: "The government's efforts to address common and pressing e-Commerce challenges are constrained by fixed resource levels. Agencies able to obtain more data on *de minimis* shipments through CBP's Entry Type 86 pilot program said they anticipate difficulties in processing a greater amount of data with their current resources. CPSC would need to explore the level of effort it would take to incorporate such data into the RAM system."[41]

---

[40] 84 Fed. Reg. 354056, Department of Homeland Security: Section 321 Data Pilot General Notice. (Tuesday Jul. 23, 2019). Available at https://www.govinfo.gov/app/details/FR-2019-07-23/context

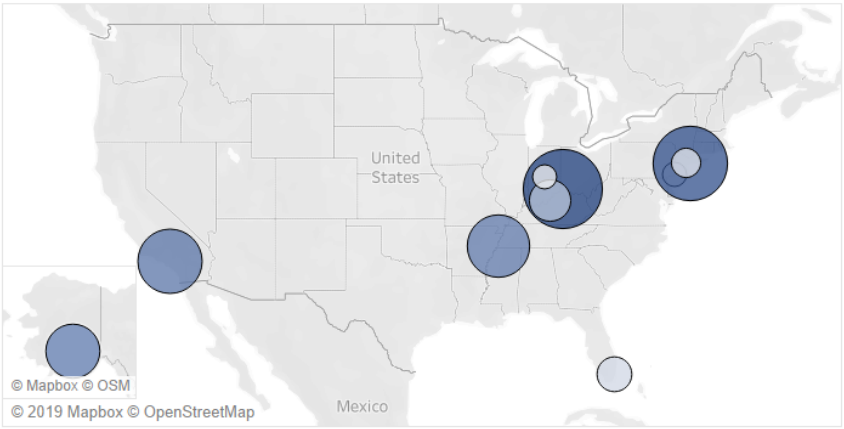
[41] CPSC e-Commerce Assessment Report, United States Consumer Product Safety Commission, Office of Import Surveillance, Nov.r 2019 at page 17. Available at: https://www.cpsc.gov/s3fs-public/CPSC%20e-Commerce%20Assessment%20Report.pdf?B.5pu7oFYPRJsokNjHygmRyZVo0tpPmE

An additional concern is data submission timing requirements for airports and land border crossings, where de minimis e-commerce normally is transported, are significantly shorter than shipments arriving via a seaport. In the case of an air, truck or rail shipment, the short window between data becoming available and the release of a shipment means CPSC staff would have little time, perhaps only hours, to target and determine whether an examination is needed. This further limits EXIS's ability to target and address imported products in those environments. The CPSC e-Commerce Assessment noted the limited time for targeting, coupled with the growth in de minimis shipments, underscores CPSC's Office of Import Surveillance's need for real-time manifest data access.

Remedying these data gaps will require changes to CBP data gathering on de minimis shipments, as well as more resources and data authority for CPSC.

STAFFING AND LOCATION GAPS: A second problem is that CPSC's Office of Import Surveillance's current staffing deployment scheme focuses on targeting larger commercial shipments that arrive in traditional seaports. (This has been a strategic deployment, as seaports have been the venue for large-value shipments of consumer goods.) In contrast, most de minimis shipments arrive via airports, express courier facilities and international mail facilities where growing numbers of e-commerce shipments arrive, but CPSC does not have staff. (An express courier facility is a specialized facility approved by a U.S. port for the examination and release of express courier shipments. Much express courier data is only available by being physically present at their facility, which is not the case for CPSC or most U.S. agencies. The CPSC e-Commerce Assessment report notes that agencies are exploring methods for receiving data from express couriers.) Effectively, CPSC's staffing model was designed before e-commerce fully emerged as a market force. Thus, CPSC's Office of Import Surveillance has a very limited presence at some express courier locations and no staff at international mail facilities.

de minimis shipments by U.S. City (CY18)



Top 10 Cities for *de minimis* Shipments (CY18)

	Number of Shipments	Percent of Total
Cincinnati	32.7M	21%
New York	29.0M	19%
Los Angeles	21.6M	14%
Memphis	20.3M	13%
Anchorage	15.3M	10%
Louisville	9.0M	6%
Miami	6.3M	4%
Newark	4.5M	3%
Philadelphia	3.1M	2%
Indianapolis	3.0M	2%
Other	8.6M	6%

CPSC's Office of Import Surveillance conducted an analysis[42] of 2018 import manifests to determine where de

[42] Id at Figure 14, page 16.

minimis e-commerce shipments are entering the United States. (City locations were considered instead of ports, because staff could theoretically act on shipments at multiple express courier ports within the same city.) The majority of cities with higher volumes of de minimis shipments are home to one or more express courier facilities, with the top five cities for de minimis shipments handling more than 75 percent of the total volume of de minimis shipments. In 2018, Jim Joholske, Director of the Office of Import Surveillance, testified to the Senate Finance Committee: "With CPSC's small size and limited resources, we currently do not have investigators stationed at locations where these small packages arrive, other than at one location at JFK airport.[43] The assessment report notes that to address this gap, CPSC should consider locating additional staff in environments where the majority of de minimis shipments are processed and assess operations at the ports receiving the most de minimis shipments and consider how staff would operate in the express and mail environments and continually adjust its port presence with respect to future e-commerce growth.

LEGAL AUTHORITY: Current consumer product safety laws do not reflect how e-commerce has significantly changed the global supply chain in recent years in a manner that has resulted in new roles not explicitly addressed in current law. The CPSC e-Commerce Assessment Report notes that current statutes can make it difficult to identify the responsibility of new parties in the supply chain and determine the extent to which these entities are, or should be, held accountable for importing non-compliant products. The CPSC's definitions of commerce participants are very broad and do not acknowledge various business models in which e-commerce participants may facilitate sales. For example, online platforms have varying degrees of ownership for the products sold through their marketplaces. Despite the significant legal implications presented by the new e-commerce participants, the CPSC has not been amended to address them. Consequently, it is not clear what level of responsibility the CPSC places on e-commerce supply chain participants. This reinforces the need to understand better and explore the varying responsibilities of all commerce participants, not just traditional actors like the Importer of Record or manufacturer.

Also notable in the CPSC report is a summary of finding from a survey of seven U.S. government agencies – CBP, USDA, FDA, Census, EPA, DOT, and the U.S. Postal Service. No agency reported that their authority has been specifically amended by Congress to address these challenges, despite widespread recognition of the need to regulate e-commerce. As well, most agencies, like CPSC, share similar gaps in acquiring data for mail and express shipments and all of the regulatory agencies are increasingly interested in obtaining access to data from the postal service and express couriers, which could provide critical targeting information for de minimis e-commerce. (Currently, CBP is the only agency with access to USPS data, but other agencies are exploring options to access and use this data for independent targeting.)

Recommendations for Enhancing Consumer Health and Safety

Given the scope and scale of threats posed to consumer health and safety in the current e-commerce environment, and the way in which those threats are generated by different factors, remedies will require changes on at least two levels.

1. Government actions

[43] Testimony of Jim Joholske, Director of Office of Import Surveillance, United States Consumer Product Safety Commission, Submitted to theU.S. Senate Committee on Finance Hearing on Protecting E-Commerce Consumers from Counterfeits, Mar. 6, 2018. Available at https://www.finance.senate.gov/imo/media/doc/06MAR2018JOHOLSKESTMNT.PDF

- CPSC: The rapid rise of e-commerce poses new challenges for CPSC since the agency does not currently have the capability to police de minimis e-commerce that enters the United States as well as it can police high-value commerce. The agency's legal, operational and resource constraints will need to be addressed. It must have the authority to hold accountable all of the parties in the e-commerce supply chain that are implicated in importing non-compliant products. CPSC's Office of Import Surveillance requires the funding to create and staff effective inspection systems that expand their presence to ensure the CPSC mission can be successful in an e-commerce context that is different in many ways from the large-value import regime to which it is now adapted, including with respect to where additional inspection staff must be fielded and new data or better data sharing between agencies developed to effectively target high-risk imports.

- FTC: The Federal Trade Commission has existing authority over unfair and deceptive practices and retail mislabeling. It is unconscionable that the FTC has not acted to discipline the big online marketplaces that claim they are not legally responsible for deceptive content on their sites, facilitate the sale of goods falsely labeled as meeting regulatory approvals or third-party certifications inspection, and in some instances do not even deliver the products presented to the consumer online. The findings of the Wall Street Journal investigation summarized earlier in this testimony provide a rich vein for FTC action, if the agency cares to engage in its mission.

- CBP: CBP has the statutory authority to inspect *any* package as it is imported into U.S. territory. Yet the agency is sitting on two slightly conflicting regulations and choosing to operate in a manner that ensures that de minimis shipments are not subject to the basic data filing requirements that would allow U.S. government agencies responsible for consumer health and safety to target high risk goods.[44] The pilot program for de minimis goods discussed previously in this testimony is a voluntary program, not a resolution to the data dodge now facilitating uninspected entry of e-commerce imports that pose high risks to consumers. As well, CBP should use its existing authority to require formal Entry for de minimis goods that it deems a high risk of evading compliance with any law or regulation. CBP has broad authority it must employ to stop and prevent the trafficking of counterfeit goods, from the assessment of civil fines and other penalties to debarring and suspending irresponsible actors. It also can and should require bonding for high-risk goods. Many of these authorities are underutilized or underdeveloped to match the risks in the evolving e-commerce environment.

- Legislating a definition of e-commerce seller: Congress must put an end to the sham of world-class retailers claiming not to be sellers and thus dodging accountability for conduct that puts consumers' health and safety at risk and unfairly penalizes legitimate businesses.

[44] Currently, the regulatory language governing the entry of merchandise subject to Section 321 provides conflicting guidance to Customs officers. The letter of 19 C.F.R. § 10.151 provides that such merchandise is to be entered under the informal entry procedures outlined in 19 C.F.R. § 143.31. But 19 C.F.R. § 143.31 provides that Section 321 merchandise require no preparation of entry at all by reference to 19 C.F.R. § 145.12. In turn, 19 C.F.R. § 145.12(d) provides that "[c]ertain types of merchandise may be passed free of duty without issuing an Entry" and refers to subpart D of part 145 for the list of such merchandise. Section 145.31 in subpart D then refers to merchandise entered under § 10.151, i.e., Section 321 entries, and requires the port director to "pass [such merchandise] free of duty and tax, without preparing an entry as provided in § 145.12." Accordingly, an apparent conflict exists between the language of § 10.151, prescribing informal entry procedures, and § 145.31, prescribing the preparation of no entry at all. In practice, Customs currently clears such goods off the manifest, meaning that it collects no information regarding the merchandise's HTSUS number.

2. E-Commerce Retailers

- Actions by companies in the e-commerce supply, distribution and sales chain will be necessary to reduce the heavy volume of counterfeit, dangerous goods to which U.S. consumers are now being exposed thanks to growing online sales. As the recent CBP report noted: "Absent the adoption of a set of best practices and a fundamental realignment of incentives brought about by strong government actions, the private sector will continue to fall far short in policing itself. Indeed, the current incentive structure tends to reward the trafficking in counterfeit and pirated goods more than these incentives help to deter such trafficking."[45] Many of the practices it recommends could reduce the platforms' facilitation of sales of fake and unsafe goods.

    - **Significantly Enhanced Vetting of Third-Party Sellers and Requirement of Insurance or Bonding or Other Forms of Security as a Condition of Access:** Platforms should only allow third-party sellers that have been vetted and approved based on a uniform assessment and proof of insurance to indemnify consumers for harm caused by their products. Assessments should include sufficient identification of the seller, its accounts and listings, and its business locations prior to allowing the seller to list products on the platform; certification from the seller as to whether it, or related persons, have been banned or removed from any major e-commerce platforms, or otherwise implicated in selling counterfeit products online or selling unsafe products; use of technological tools, as well as analyses of historical and public data, to assess risk of sellers and products; and establishment of an audit program for sellers, concentrating on repeat offenders and those sellers exhibiting higher risk characteristics. Any failure to provide accurate and responsive information should result in a determination to decline the seller account and/or to hold the seller in violation of the platform's terms of service.

    - **Pre-Sale Identification of Third-Party Sellers and the Rule of Origin of the Good for Sale:** Providing consumers with this information up front as part of the first screen available for a product is critical for consumers to make informed choices.

    - **Set <u>and Enforce</u> Limitations on High Risk Products:** Platforms should have in place protocols and procedures to place limitations on the sale of products that have a higher risk of posing threats to public health and safety. For example, some major platforms completely prohibit the sale of prescription medications by third-party sellers in their marketplaces. Many platforms also ban the sale of products that are known to pose a safety risk when sold online. Examples include car airbag components, infant formula and new batteries for cellphones. But these terms, which are included on platforms on which prohibited and restricted goods regularly appear, are only effective if enforced by the platform through an investment in regular surveillance and monitoring and the development of automated tagging systems that keep unsafe products from reappearing on sites.

    - **Effective Takedown Procedures for Unsafe Goods:** Platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns for unsafe goods and protocols to ensure goods are not relisted.

[45] Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States, Department of Homeland Security, Jan. 24, 2020 at page 26. Available at https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf