July 29, 2019

BY ELECTRONIC FILING

Mr. Stevan Mitchell
Director
Office of Intellectual Property Rights
International Trade Administration
U.S. Department of Commerce
1401Constitution Avenue NW, Room 21028
Washington, DC 20230

Re: Request for Comments Regarding the Report on the State of Counterfeit and Pirated Goods Trafficking and Recommendations [Docket No. DOC-2019-0003]

Dear Mr. Mitchell,

In response to the Department of Commerce's request for comments from intellectual property ("IP") rights holders, online third-party marketplaces, other third-party intermediaries, and other private-sector stakeholders on the aforementioned notice, the National Retail Federation ("NRF") respectfully submits these comments and suggestions.

NRF is the world's largest retail trade association. Based in Washington, DC, NRF represents discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and internet retailers from the United States and more than 45 countries. Retail is the nation's largest private-sector employer, supporting one in four U.S. jobs — 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

In these comments, which address each of the eight questions listed in the Department of Commerce's request for comments in turn, NRF highlights the negative impacts of the increasing

prevalence of counterfeit goods in the marketplace and provides suggestions and recommendations that, if adopted by the Department of Commerce and Department of Homeland Security, would help curb the trafficking of counterfeit and pirated goods.

QUESTION 1: How are your interests affected by counterfeit or pirated goods imported through online third-party marketplaces and other third-party intermediaries as those terms are defined in the presidential memorandum?

While it is impossible to enumerate all of the ways in which counterfeit and pirated goods imported by various third-party intermediaries affect retailers, the harm is felt most acutely in terms of brand reputation, financial health, and customer relations.

Brand reputation becomes an immediate casualty when customers unknowingly spend their hard-earned dollars on goods sold at brick-and-mortar retail stores or on online third-party marketplaces, only to later discover that these goods are shoddy or inferior counterfeits. Customers defrauded by counterfeit or pirated goods may lose faith in the brand they have grown loyal to, and in turn, the reputation that brands have spent years and countless resources to establish suffers irreparable damage. The harm caused by one marketplace's inadvertently carrying the counterfeit or pirated goods claiming to be associated with a particular brand is difficult to contain and can affect the reputation and sales of that brand's products no matter where they are sold.

In addition to the damage suffered by owners of the IP rights, third-party retailers are significantly injured by the growing prevalence of counterfeit and pirated products. Retailers are, after all, customer-centric businesses that, when taken advantage of by those trafficking in counterfeit or pirated goods, inadvertently provide valuable space, either online or at retail stores,

for individuals seeking to defraud their customers. Retailers, whether they sell their own brands of goods or those of others, spend countless resources establishing reputations with their customers. A customer's experiencing even a single instance in which he or she buys a counterfeit product off the shelf or website of a retailer can thus undermine a customer's trust in the retailer as much the brand of the product.

Financially, the importation of counterfeit and pirated goods also harms retailers through diverting both sales and resources that are essential to the health and continued growth of retail businesses. Counterfeit goods hurt the bottom line of retailers carrying genuine products from respected brands as millions of dollars of potential sales are lost and diverted to individuals hawking counterfeit and pirated products. Faced with this reality, retailers seeking to guarantee the quality of their products are forced to spend valuable time and resources on efforts to both prevent counterfeit and pirated goods from reaching their shelves and address issues with customers and suppliers when counterfeit or pirated goods are discovered. Small and new businesses are most vulnerable to these harms as they often have the least resources, access to information, and experience necessary to vet products and verify sellers. Similarly, instances in which one e-commerce platform engages in selling counterfeit or pirated goods threatens the reputation of all e-commerce platforms generally.

The growing prevalence of counterfeit and pirated goods also threatens customer safety. Individuals trafficking in counterfeit or pirated goods will use deceptive practices and copy trademarked material to sell unwitting customers goods that may not meet safety protocols or specifications. In June 2019, the EUIPO published a report entitled "2019 Qualitative Study on

Risks Posed by Counterfeits to Consumers", which found that 97 percent of recorded dangerous counterfeit goods were assessed as posing a serious risk, and that the end users of 80 percent of the goods reported to be dangerous and counterfeit were for children (e.g., toys, childcare items and children's clothing).

Question 2: What factors contribute to trafficking in counterfeit and pirated goods through online third-party marketplaces or other third-party intermediaries, and what market incentives and distortions may contribute to the use of online third-party marketplaces and other third-party intermediaries to traffic in counterfeit and pirated goods?

Several factors contribute to trafficking in counterfeit and pirated goods through online third-party marketplaces or other third-party intermediaries. One factor is the lack of sufficient enforcement by government agencies when it comes to policing counterfeit imports. In general, government agencies, including Customs and Border Protection ("CBP"), lack the resources and data they need to prevent the growing volume of imported counterfeit and pirated goods from entering the U.S. market, and counterfeiters know and exploit it. For instance, CBP recently noted that it "does not receive adequate advance information in order to effectively and efficiently assess the security risk of the approximately 1.8 million Section 321 shipments that arrive each day."[1] In addition, there has been insufficient information sharing and coordination among the agencies responsible for implementing and enforcing anti-counterfeit measures, further contributing to the proliferation of counterfeit and pirated goods on online marketplaces. In addition, government agencies tend to provide only limited information about the seizure of counterfeit and pirated goods and the identity of the involved sellers and importers to third party

[1] See https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-15625.pdf?utm_source=federalregister.gov&utm_medium=email&utm_campaign=pi+subscription+mailing+list.

marketplaces and IP rights holders, and when information is provided, it is often delayed. Agencies have also not provided any guidance to marketplaces on best practices for detecting counterfeit and pirated goods.

Third party marketplaces have had difficulty responding to the problem of counterfeit and pirated goods for many of these reasons. For example, with no reliable, consistently updated source of information about third party sellers or seized shipments, marketplaces face difficulties vetting sellers, responding quickly when counterfeit and pirated goods sellers are detected by relevant government enforcement agencies, and preventing online sellers from avoiding detection. Meanwhile, sellers of counterfeit and pirated goods that face ejection from one platform can often leap to another platform while avoiding detection. As a result, third-party marketplace policies and practices remain primarily reactive in responding to the discovery of counterfeit and pirated goods and holding unauthorized sellers accountable. Further exacerbating this state of affairs is a lack of coordinated effort amongst competing marketplaces; if all marketplaces are not working together and adopting common best practices, sellers of counterfeit and pirated goods will be able to exploit differences in policy and lack of coordination to avoid detection.

QUESTION 3: Are there effective technologies, the use of which—by the private sector and/or law enforcement agencies—could substantially reduce the sale and importation of counterfeit and pirated goods through online third-party marketplaces and/or enable more effective law enforcement regarding the trafficking in such goods? Please reference and provide copies of any available studies that demonstrate the efficacy of such technologies, or any available data that may be used to do so.

There are several existing technologies that would help both law enforcement and the private sector quickly identify counterfeit and pirated products. Some retailers have utilized

software that monitors sellers online and third party marketplaces for unauthorized sellers and counterfeit and pirated goods. Another software used by some IP rights holders collects data and images on goods and sellers from across numerous online marketplaces to determine if sellers are listing goods online without the brand's authorization or if sellers listing counterfeit or pirated goods are working across multiple platforms. Retailers aided by these tools have reported dramatic increases in the number of takedown requests they have sent to online platforms.

The software's primary weakness, however, is that the information is not updated by the government in real-time, meaning that several weeks may pass before counterfeit sellers or goods are discovered and removed from online marketplaces. Delays of that length during the holiday season can result in a large quantity of counterfeit or pirated goods escaping detection, harming both consumers and retailers. In addition, retailers using this kind of software bear significant costs associated with these products, while the effectiveness of their efforts are undermined by others that do not implement similar measures.

QUESTION 4: To what degree can expanded collaboration and information sharing among online third-party marketplaces, other third-party intermediaries, intellectual property rights holders, other private-sector stakeholders and/or U.S. law enforcement organizations substantially reduce trafficking in counterfeit and pirated goods and/or enable more effective law enforcement regarding the trafficking in such goods?

Expanded collaboration and information sharing among online third party marketplaces, third party intermediaries, IP rights holders, other stakeholders, and U.S. law enforcement agencies could substantially reduce trafficking in counterfeit and pirated goods. While collaboration in information sharing should be voluntary, government agencies can play a central

role in encouraging collaboration and participation by all stakeholders by improving and centralizing information sharing.

NRF envisions and supports the development of a collaborative, voluntary information sharing system through which IP owners, retailers, other third party intermediaries, as well as government agencies can contribute to and access a centralized, up-to-date source of data about seizures of counterfeit or pirated goods. This system should include information from U.S. agencies provided in real time and should be sufficient to inform IP rights owners of the seizures of suspect goods and enable third-party marketplaces to identify suspect sellers, remove counterfeit and pirated goods from the marketplace, and address customer concerns quickly. In conjunction with these data sharing efforts, training and resources should be provided to CBP agents as well as industry stakeholders to help relevant personnel flag suspicious products.

With an improved system for accessing information collected by government agencies, private sector stakeholders could pursue further collaboration through, for example, crafting best practices for dealing with counterfeit and pirated goods. CBP's recently announced Section 321 Data Pilot Test exemplifies the kinds of data collection efforts that could help inform private sector stakeholders of risks associated with counterfeit and pirated goods. As part of the pilot, CBP plans to collect advance information from regulated and non-regulated entities, such as online marketplaces, and require the submission of additional data that identify the entity causing the shipment to cross the border, the product in the package, the listed marketplace price, and the final recipient. NRF is supportive of the pilot, which seeks to address the growing prevalence of

counterfeit or pirated goods while still recognizing the value of efficiency afforded by the Section 321 designation.

QUESTION 5: Are there federal agency data collection or standardization practices, or practices involving provision of data to parties, that could promote more effective detection, interdiction, investigation or prosecution of underlying violations of U.S. customs laws and of intellectual property rights?

As previously noted, improved information sharing and collaboration can play a central role in reducing trafficking in counterfeit and pirated goods. CBP and other Partner Government Agencies should promptly collect and share information when counterfeit or pirated products are seized and notify the relevant stakeholders. At a minimum, IP rights holders need to be able to determine the importer and exporter's name and address to adequately respond when they discover counterfeit goods. With this in mind, CBP should provide additional information to stakeholders, such as the importer of record or the FBA number on shipments. This information would help IP rights holders, third party marketplaces, and other stakeholders more effectively identify and remove counterfeit and pirated goods and their sellers from the market. Other helpful information that CBP should provide to stakeholders include: the volume of goods seized, images of the goods at issue, and the markings, alphanumeric symbols, and other coding appearing on the goods and their retail packaging.

CBP's recently announced Section 321 Data Pilot Test, noted above, exemplifies the kinds of efforts to obtain relevant data for countering the sale of counterfeit and pirated goods that are a step in the right direction. If utilized properly, these kinds of programs can better inform private sector stakeholders of the risks and assist CBP and other agencies in designing risk-based targeting systems. NRF also believes that more research can be done on applying

emerging technologies to assist in verifying the source of goods and identity of sellers. For instance, the use of block chain technology should be studied as a possible solution for recording and verifying the chain of custody of goods sold online and in retail outlets.

QUESTION 6: What existing policies, procedures or best practices of online third-party marketplaces, other third-party intermediaries, intellectual property rights holders, and/or other private-sector stakeholders have been effective in curbing the importation and sale of counterfeit and pirated goods, including those conveyed through online third-party marketplaces?

Several of the country's largest e-commerce platforms have instituted programs that have proven effective in verifying legitimate sellers, identifying and removing counterfeit and pirated products from their platforms, and helped IP rights holders obtain information to identify infringing sellers.

Walmart.com's Marketplace is a closed marketplace where prospective sellers must initially satisfy a number of criteria to be approved to sell items on http://Walmart.com. The criteria for prospective sellers includes a risk based vetting of seller applications, including vetting key information such as the seller name, business name, physical address, email address, websites, and tax ID number. Walmart also requires prospective sellers to disclose international business ownership and any product fulfillment outside of the United States. Sellers who want to sell in categories with more counterfeit risks require additional vetting before they are allowed to sell items in these specific categories.

eBay's VeRO program has been noted for its progress in identifying and removing counterfeit products. Other programs, such as Amazon's Brand Registry program, provide IP

rights holders with information so that they can determine if products are being sold without authorization and, if necessary, issue cease and desist letters to infringing sellers.

IP rights holders themselves have also conducted test purchases of items suspected of being counterfeit or pirated. This practice enables holders to obtain information about the seller's identity, location, and potential links to other seller accounts engaged in trafficking of counterfeit or pirated goods, as well as information about who is manufacturing them.

Alibaba launched the Alibaba Anti-Counterfeiting Alliance ("AACA"), which includes over 132 brands as members. The AACA collaborates on six key initiatives: 1) proactive online monitoring and protection, 2) a product test-buy program, 3) offline investigations and enforcement actions, 4) industry-law enforcement workshops, 5) litigation tactics, and 6) public awareness campaigns. Members are divided into twelve industry working groups and are able to share feedback in areas such as IPR enforcement-related strategies, new trends, and litigation and platform practices throughout the e-commerce industry. The AACA has also created an intellectual property protection portal through which IP rights holders can report suspect listings and share information with the company and a Good-Faith Program that provides faster take down for brands with a track record of accurate notice and take-down filings.

QUESTION 7: What additional policies, procedures or best practices of online third-party marketplaces, other third-party intermediaries, intellectual property rights holders, and/or other private-sector stakeholders can be effective in curbing the importation and sale of counterfeit and pirated goods, including those conveyed through online third-party marketplaces? What would it cost for industry to adopt such practices?

Online third party marketplaces can adopt vetting and verification procedures that, at a minimum, are able to:

- verify that the user seeking to establish a seller account is a real person;
- confirm that the user seeking to become a seller has no history of selling, distributing, or trafficking counterfeit or pirated goods; and
- locate and provide notification for individuals identified as selling, distributing, or trafficking counterfeit or pirated goods.

Third party marketplaces can also adopt procedures that hold those who traffic in counterfeit and pirated goods responsible. These policies and procedures should:

- ensure that takedown requests are addressed promptly when they are issued by IP rights holders. This may involve creating a trusted portal for verified rights holders;
- inform customers about counterfeit and pirated goods and to help customers determine if goods they have purchased are in fact counterfeit or pirated;
- release annual reports that contain information about the number of instances involving the sale of counterfeit and pirated goods and the marketplace's response; and
- create partnerships with payment processors to notify them when a seller is terminated from an online marketplace.

Third party marketplaces should also voluntarily adopt policies and procedures to make more information about sellers available to consumers. Consumers navigating through third party online marketplaces can easily read about and review products themselves, but few allow customers to obtain information about the legitimacy or track record of a seller or other

customers' experiences with that seller. Improving transparency on third party marketplaces in this manner would nurture a better functioning market by allowing consumers to make informed decisions not only about what they purchase, but also from whom they purchase.

Third party intermediaries, including express carriers, may help curb or prevent trafficking in counterfeit and pirated goods by adopting policies and procedures that:

- ensure personnel handling packages and shipments have sufficient training, resources, and technology to effectively detect and flag shipments and packages potentially containing counterfeit or pirated products;
- collect and centralize information storage obtained from customers that can be provided to, and analyzed by, trusted private sector stakeholders – including third party market places and IP rights holders when necessary – to investigate potential trafficking in counterfeit or pirated goods; and
- report information about suspected packages to relevant enforcement agencies and private sector stakeholders, including data that helps identify the source and destination of counterfeit and pirated goods.

Third party intermediaries including shipper and freight forwarders should collaborate with third party marketplaces and IP rights holders to establish common product verification protocols, reporting requirements, and data collection and sharing standards. This collaboration should be established as a Trusted Shipper Program that would periodically certify the compliance of shippers, freight forwarders, and other intermediaries involved in the importation of products for third party marketplaces. A program like this would ensure shippers and other

intermediaries are employing consistent, best practices to help prevent counterfeit goods from entering markets. An initiative like this would also increase confidence of third party marketplaces, IP rights holders, and consumers that intermediaries are doing their part to prevent and address trafficking in counterfeit or pirated goods.

QUESTION 8: What policy remedies, including administrative, regulatory, or legislative changes by the federal government (including enhanced enforcement actions) could substantially reduce the trafficking in counterfeit and pirated goods and/or promote more effective law enforcement regarding the trafficking in such goods? Please reference any available analyses that shed light on the efficacy and potential impacts of such proposed remedies?

Agencies such as CBP and the United States Patent and Trademark Office would benefit from increased resources, both in terms of technology and human resources, to help flag suspicious goods, collect and share information about sellers, and enforce the rights of IP rights holders. The U.S. government should also provide guidance tailored to industry stakeholders as well as consumers on tackling the problem of counterfeit and pirated goods. As the increasing prevalence of counterfeit goods demonstrates, shipping channels remain vulnerable to exploitation by bad actors, and a robust, whole-of-government approach in which well-resourced agencies work collaboratively with one another and with stakeholders on data tracking, collaboration, and enforcement is necessary.

The Federal Trade Commission ("FTC"), working with agencies involved in the protection of human health and safety (e.g., the Consumer Product Safety Commission, the Food and Drug Administration), should also issue guidance for consumers to improve their awareness of: 1) the risks of counterfeit or pirated goods, and 2) ways to identify suspicious sellers and products on third party marketplaces. Educational campaigns aimed at improving consumer

knowledge and awareness should be done in a coordinated manner among the relevant agencies so that there is a consistent, whole-of-government approach. Such efforts should include: disseminating guidance and other relevant materials online; creating webinars for consumers that explain best practices for identifying and avoiding counterfeit or pirated products; and posting informational e-flyers on targeted websites. The FTC's successful campaign aimed at educating consumers regarding gift card fraud should be instructive in crafting and executing a strategy for these efforts.

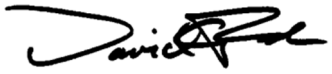
CBP, the Department of Homeland Security ("DHS") and the U.S. Postal Service ("USPS") must also improve its enforcement capabilities with respect to existing laws if it hopes to make any progress on countering trafficking in counterfeit or pirated goods. These agencies' poor performance in implementing and enforcing the STOP Act, a law specifically aimed at enhancing oversight and data collection on shipments sent into the U.S. from abroad, underscores the need to focus greater resources on actual enforcement. For example, USPS was required under the STOP Act to have Advanced Electronic Data ("AED") on 100 percent of packages from China and 70 percent of packages from foreign posts overall by the end of last year. Nevertheless, USPS reported to congress that for 2018, it collected AED on only 70 percent of packages from China and 52.8 percent overall. DHS's OIG report on STOP Act enforcement found that "CBP operations at JFK [Airport] were only able to inspect a "limited number of the hundreds of thousands of pieces of incoming mail" at JFK per day. As reports on the STOP Act's enforcement have illustrated, government agencies must do more to develop the capabilities required to curb the rise of counterfeit and pirated goods.

In addition, as CBP continues its 321 Data Pilot Test, the agency should evaluate the effectiveness of allowing 321 entries through U.S. Foreign Trade Zones (FTZ). These informal entries are not currently allowed through a U.S. FTZ. Modifying U.S. law to provide de minimis entry eligibility for products withdrawn from U.S. FTZs would encourage e-commerce distribution growth from already compliant U.S. FTZs. It would also reduce the risk of counterfeit, infringing, and illicit goods from entering the U.S. Customs territory, given CBP's enhanced enforcement ability for FTZs.

* * *

Thank you for the opportunity to submit comments on this very important topic. NRF would be pleased to discuss these comments with the Department if it would be helpful and to participate in any follow-up meetings or events that the Department may host to discuss potential next steps.

Respectfully submitted,



David French
Senior Vice President
Government Relations