IACC
INTERNATIONAL ANTICOUNTERFEITING COALITION

Submission of the
International AntiCounterfeiting Coalition
to the
Department of Commerce

Report on the State of Counterfeit and Pirated Goods Trafficking and Recommendations
Request for Public Comment
84 Fed. Reg. 32861 - 63 (July 10, 2019)

July 29, 2019

---

727 15th Street NW • 9th Floor • Washington, DC 20005 • USA • +1(202)223-6667 • iacc@iacc.org • www.iacc.org

The International AntiCounterfeiting Coalition, Inc. ("IACC"), is pleased to submit these comments to the Department of Commerce ("the Department" or "Commerce"), pursuant to the request published in the Federal Register on July 10, 2019, seeking written comments from the public concerning "the state of counterfeit and pirated goods trafficking through online third-party marketplaces and recommendations for curbing the trafficking in such counterfeit and pirated goods."

The IACC is the world's oldest and largest organization dedicated exclusively to combating trademark counterfeiting and copyright piracy. Founded in 1979, and based in Washington, D.C., the IACC represents more than 200 corporations, trade associations, and professional firms, spanning a broad cross-section of industries. IACC members include many of the world's best-known brands in the apparel, automotive, electronics, entertainment, luxury goods, pharmaceutical, personal care, software, and other consumer product sectors.

Central to the IACC's mission is the education of both the general public and policy makers regarding the severity and scope of the harms caused by the illicit trafficking of counterfeit and pirated goods. The IACC seeks to address these threats by promoting the adoption of legislative and regulatory regimes, as well as industry best practices, to effectively protect intellectual property rights, and to encourage the application of resources sufficient to enforce those rights. The IACC works with U.S. and foreign government partners and private sector stakeholders throughout the world to identify, and to seek remedies to, legislative deficiencies and practical impediments to IP enforcement. The IACC has also led the development of voluntary collaborative programs on a global scale to address key priorities in the online space, including its RogueBlock, IACC MarketSafe, and MarketSafe Expansion programs.

Whether measured in terms of sales lost by legitimate manufacturers and retailers to illicit competitors, tax revenues and duties that go unpaid to governments, decreased employment, or diminished investment in capital improvements and research and development; counterfeiting is a significant drain on the U.S. and global economy. Further, the production and distribution of goods manufactured in an entirely unregulated supply chain, where the makers have every incentive to cut corners by using cheap, substandard components, and no incentive to abide by accepted standards of consumer health and safety, presents a clear threat to the health and well-being of consumers, and to the integrity of our national security infrastructure. We look forward to working with you to ensure the safety of consumers and the vitality of legitimate manufacturers and retailers impacted by the global trade in counterfeit and pirated goods.

For clarity's sake, Section I of this submission is organized as a series of responses to the questions enumerated in the Request for Comments. Additional comments deemed relevant to the Department's inquiry, concerning the IACC's ongoing programs, are set forth in Section II of this submission. Further, in light of the Department's stated intent to consider previous

public submissions, including the USTR's annual Special 301 Report and Review of Notorious Markets, Section III of this filing highlights and provides links to several past public submissions relevant to the present inquiry.

I. RESPONSES TO THE DEPARTMENT'S ENUMERATED QUESTIONS

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?

The terms "global commerce" and "e-commerce" have become increasingly synonymous in recent years. And as both legitimate retailers and consumers have turned to online distribution channels, the manufacturers and sellers of illicit goods have likewise followed suit. Across every sector of the IACC's membership, the need to address the trafficking of counterfeit and pirated goods in e-commerce has been cited as a top priority. The vast amounts of resources our members must dedicate to ensuring the safety and vitality of the online marketplace, bears out the truth of the issue highlighted by Peter Navarro, Assistant to the President for Trade and Manufacturing Policy, in his April 3, 2019 Op-Ed piece in The Wall Street Journal - that the sale of counterfeit brand-name goods presents a pervasive and ever-growing threat in the online space. One IACC member reported making hundreds of investigative online test purchases over the past year, with a nearly 80% successfully resulting in the receipt of a counterfeit item.

The harms caused by online trafficking are varied, but well-established. In many cases they're no different than those seen historically within the brick and mortar context: sales of counterfeits displace legitimate sales by manufacturers and retailers, and the distribution of substandard knock-offs diminish brands' reputations and destroy the goodwill associated with their trademarks. In turn, IP owners are deprived of the just fruits of their labors, and left with fewer resources to compensate their employees and hire new ones; their ability to invest in capital improvements is diminished; and their contribution to the tax base is reduced. They're also forced to divert resources away from their real business in what often seem to be never-ending efforts to maintain a reasonably-level playing field with the illicit competitors who seek to unfairly profit off of rights-holders' innovations and reputations. The online trafficking of counterfeit and pirated goods however also raises some unique challenges above and beyond those seen in the traditional brick and mortar distribution chain; those factors are discussed in greater detail below.

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?

As detailed in a report published last January by the Government Accountability Office[1], sellers of counterfeit goods are increasingly seeking to exploit legitimate e-commerce services to reach unwitting consumers. Online marketplaces are attractive targets for counterfeiters for a variety of reasons – among them, that consumers' familiarity with the platforms, and the goodwill and trust imbued by that familiarity, may extend to the individual sellers on the platform. Consumers, to some extent, appear not to distinguish between buying directly from the platform itself or from a third-party seller on the platform – a fact that may be exacerbated by the way listings for goods are presented to prospective buyers. Listings may be displayed in a standardized format, with stock photos (or in some cases with photos of the authentic goods, lifted directly from trademark owners' own catalogs or websites without authorization), with relatively minor distinctions between individual sellers that are often not readily apparent to shoppers. Likewise, consumers' interactions with sellers are frequently carried out entirely through the platform, with all aspects of the transaction, from research to sale, processing of payment, shipping logistics, and post-sale complaints mediated by the platform.

The relative anonymity of e-commerce sellers contributes not only to consumer confusion though, it also makes it increasingly difficult for rights-holders to take effective and lasting action against counterfeiters, and indeed for e-commerce platforms themselves to know with certainty with whom they're doing business. The onboarding and vetting of sellers remain a concern of the highest priority for rights-holders in addressing the trafficking of counterfeits online. While the brick and mortar economy has a well-developed regulatory regime for the licensing and oversight of sellers, a comparable regime is largely non-existent in the online realm. Many online marketplaces lack any effective mechanism for verifying the identity of sellers or their ability to source (authentic) goods that they're purporting to make available to consumers. The lack of relevant policies and procedures to verify sellers' true names and addresses, and to conduct similar due diligence, in turn, contributes to a range of other impediments to effective enforcement. Absent those sorts of checks, sellers can easily establish multiple alias accounts to skirt disciplinary actions taken by platforms for IP violations, or maintain seemingly unrelated operations across multiple platforms. It should not be surprising then that some of the most frequent complaints heard from IACC members involve recidivism by counterfeiters that is enabled precisely by such strategies.

The absence of appropriate vetting procedures for sellers during the onboarding process – and as an ongoing matter – feeds into and compounds rights-holders' concerns regarding the largely reactive approach to IP enforcement on e-commerce platforms. While many platforms engage in some degree of pro-active enforcement, there is a great deal of disparity among platforms with regard to such efforts; and historically, enforcement has followed a notice-and-takedown procedure that places a heavy burden on legitimate manufacturers and retailers to police their intellectual property. This approach has been largely necessitated by court rulings that have narrowly construed platforms' duty to act against listings for counterfeits to those cases in which the platforms have actual knowledge of illegal activity. While the operators of e-commerce platforms may justifiably argue that they lack the expertise to authoritatively determine whether the goods offered by a third-party seller are authentic or counterfeit, rights-

[1] Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market, GAO-18-216, January 2018. https://www.gao.gov/assets/690/689713.pdf.

holders' efforts have often devolved into an endless cycle of takedown requests. A request is submitted and actioned by the platform, after which the seller simply re-lists the same goods for sale using the same or another account that they operate on the same platform, or they migrate to another platform, and the cat-and-mouse game continues. Appropriate vetting and monitoring of sellers, in conjunction with terms of service that treat IP violations as serious offenses and punish such violations accordingly are essential components to addressing the sorts of recidivism that rights-holders experience on e-commerce platforms.

The challenges experienced by rights-holders and law enforcement in e-commerce are not limited to third-party marketplaces, however. The evolution of the distribution chain for counterfeit goods in response to the explosion of online sales in recent years has presented a range of difficulties for enforcement by the public and private sector. Historically, the counterfeit goods distributed within the U.S. market have been sourced from overseas, primarily from China, and transported to the United States via large-scale shipments as ocean cargo. Retail distribution was centered in flea markets, swap meets, and informal street vendors, which were reliant upon larger scale importation, warehousing, and wholesaling operations. This intermediation provided a number of choke-points in the supply chain, each of which offered substantial opportunities for impactful enforcement and the substantial reduction of inventory available in the market. While China remains far and away the greatest source of counterfeit goods available to U.S. consumers, the e-commerce distribution model has greatly diminished the potential impact of enforcement actions.

As detailed in the annual IPR seizure statistics published by U.S. Customs and Border Protection ("CBP"), the growth in e-commerce we've seen in recent years correlates with a massive increase in the number of IPR-related seizures in the international mail and express consignment environments. Counterfeiters are no longer forced to rely on in-country intermediaries to facilitate their sales to U.S. consumers; their online presence – whether on an e-commerce platform, a standalone website, or a social media account – is the modern day flea market stall, and their illicit wares are carried straight to consumers' front doors by the postal service or express delivery companies. The impact of this new paradigm is felt in two distinct ways. First, CBP has been overwhelmed with a flood of small consignments that significantly strain its ability to effectively target and interdict counterfeit imports. Concurrently, even successful interdictions have a miniscule impact on the overall availability of counterfeits in the market (both in absolute terms and in comparison to the container-load seizures that were more typical in the past). And because the counterfeiter has already been paid for such seized shipments, the deterrent effect of such actions against future sales is greatly diminished.

A final contributing factor to the growth in the trafficking of counterfeits via e-commerce, and one that should not be discounted in terms of its importance, is the continued lack of recognition among consumers about the scope and scale of counterfeit sales online, even on major e-commerce platforms. Despite significant efforts by rights-holders and other stakeholders, including government-led actions such the aforementioned 2018 GAO report, the annual Notorious Markets review, and the DHS-led Operation In Our Sites; public awareness regarding the risks associated with counterfeits in e-commerce remains troublingly low, and price often remains a determinative factor in consumer behavior online.

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.**

The IACC's brand-owners and content producers invest heavily in the use of technologies to abate the trafficking of counterfeit goods and pirated content; likewise, the IACC's product security and brand protection service providers develop and implement technological solutions to combat illicit trafficking and importation in a variety of ways. By way of example, one IACC member noted its adoption of software used to monitor sellers on a large number of third-party marketplaces, enabling it to scrape and analyze data to identify infringing uses of its intellectual property (e.g., copyrighted images stolen from their websites and catalogs) and offers for counterfeit versions of its products. Within a month of its use of these tools, its confirmed identification of listings for counterfeit goods increased by approximately 500%. Such technologies are used widely by IACC members and other rights-holders, and have become to a great extent necessary for companies both small and large to identify targets for investigation given the overwhelming volume of goods on offer through e-commerce platforms.

In the trade enforcement context, technological tools have been widely adopted by rights-holders, who typically employ a multi-layer approach incorporating both overt and covert technologies to improve the efficiency of authentication at the border and to ensure the accuracy of such authentications. Overt technologies may include something as simple as a unique serial identification number, watermarks, labels with color-shifting inks or holograms, or similar features. Covert technologies meanwhile often include the use of encrypted codes, markings, or tags not readily apparent by visual inspection, and which may require the use of proprietary scanners or make use of smartphone apps and the like to read and decrypt the tags, or to confirm its authenticity against a proprietary database. The layered use of covert and overt technologies significantly diminishes the ability of counterfeiters to make a product or packaging that will pass muster when examined by an individual possessing the relevant expertise.

Ultimately, the goal of all of these technologies is to improve the efficiency of enforcement; to that end, and keeping in mind Customs' dual mandate of trade facilitation and trade enforcement, speed and accuracy are essential. Many rights-holders and their service providers are exploring the use of artificial intelligence and machine learning to advance these efforts; given the rapid pace of developments in these areas, and the incredible range of technologies currently available in the marketplace, we believe that the establishment of an advisory group to ensure our public sector counterparts' awareness and understanding of the tools available, their capabilities, and limitations, should be considered.

Regrettably, the effectiveness of such technologies has been greatly hampered by CBP's reluctance to seek assistance from, and to share information with, rights-holders prior to seizure. As outlined in prior IACC filings, CBP has insisted that its authority to disclose information to rights-holders is restricted by the Trade Secrets Act. Congress has spoken to the issue with its enactment of Section 818(g) of the National Defense Authorization Act for Fiscal Year 2012, specifically providing for the disclosure of information found on the product

and its packaging, and including unredacted digital images of the goods. In response however, CBP adopted an ungainly amended regulation prohibiting the provision of such information and of unredacted images until after the importer was given a seven-day period to provide evidence of the goods' authenticity. That waiting period appears to have been created out of whole cloth and lacking any statutory basis; it has long been viewed as simply decreasing the efficiency of the process and preventing timely assistance from rights-holders that might promptly resolve the question of the goods' authenticity.

Congress revisited the issue three years ago, including provisions in the Trade Facilitation and Trade Enforcement Act of 2015 (Sec. 302) ("TFTEA") which superseded the NDAA provisions. Again, Section 302 explicitly authorized CBP to seek assistance from persons as necessary to determine whether the importation of certain goods would violate the statutory prohibitions on importing goods in violation of IP rights. Importantly, the definition of "person" was limited to rights-holders, and excludes any mention of seeking assistance from importers for such purposes.

Similarly, the Administration's Executive Order 13785 of March 31, 2017, directed CBP to develop and implement a plan within 90 days – to include undertaking a rulemaking, if necessary – to ensure that the agency could share information with rights-holders as necessary to determine whether an importation would violate U.S. law.

The way in which CBP chose to implement the NDAA, and its failure to implement the authority provided by both the TFTEA and the Executive Order, has led to frequent reports from rights-holders regarding difficulties in providing effective assistance to CBP in carrying out its IP enforcement mandate. With proper implementation, legitimate manufacturers could provide the sort of assistance necessary to enable the expeditious determination of a product's authenticity from digital images of a product and its packaging, as well as the identification of the importer, exporter, and quantity of goods seized, significantly improving the efficiency of examinations. Without it however, many of the investments in technological tools cannot currently be effectively leveraged in a timely manner.

With regard to pirated content, the importation of such goods has largely shifted to a digital paradigm – the goods themselves are simply downloaded. But in many cases, those digital files are useless unless the end-consumer has obtained a circumvention device necessary to bypass the rights-holders' technological protection measures or access controls. The importation of circumvention devices is already prohibited under federal law, but enforcement against the manufacturers, exporters, and importers who supply the consumer market remains difficult, as relevant rights-holders have to date been unable to obtain information regarding shipments of circumvention devices seized or detained by CBP comparable to that provided in seizure notices to trademark and copyright owners. Section 303 of the TFTEA authorized CBP's disclosure of such information, yet over three years later, that authority also has not been implemented.

The common thread that connects the use of technological tools for IP enforcement and what ultimately determines its effectiveness – both online and at the border – is accurate and verifiable data. Whether in terms of pro-active efforts by platforms to monitor and remediate illicit sales through their systems, efforts of brands or law enforcement officials to confirm the true provenance of goods identified by a trademark, or to draw connections between an online presence and individuals' or organizations' real-world manufacturing, financial, or logistics

operations – data is the key. Unfortunately, that data is often compartmentalized or siloed by stakeholders, hindering more in-depth analysis that could lead to more effective and efficient enforcement. As discussed in greater detail below, the IACC has focused heavily on data sharing as a foundation of its own enforcement programs, seeking to leverage intelligence from partners across industry sectors to more effectively target counterfeiting operations.

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?**

As discussed herein, and in numerous other public submissions, the IACC strongly supports an approach to enforcement that prioritizes collaboration and information sharing to combat the trafficking of counterfeit and pirated goods. It's often said that "we cannot arrest our way out of the problem." While we concur with that statement, that leaves perhaps only one realistic option – making it impossible for counterfeiters to continue doing business. Doing so will not be feasible however, as long as the remedial actions taken in response to violations remain fractured in terms of their implementation.

Returning to the previously discussed issue of recidivism among online sellers, the continued operation of bad actors across multiple platforms, and their ability to simply migrate from one platform to another in response to enforcement actions by the platforms, simply results in a new variation on the traditional "whack-a-mole" model that has plagued online enforcement since the outset. Expanded collaboration and information sharing among online third-party marketplaces, coupled with the adoption of effective "know your customer" procedures, and a commitment by e-commerce platforms to take reasonable steps to monitor the commercial activities of sellers on their platforms who have a history of violations on their own or other platforms, could substantially reduce trafficking in counterfeit and pirated goods. Further, we would encourage platforms to take additional steps to inform rights-holders about the pro-active and responsive actions they've taken against sellers of illicit goods; and in doing so, to provide all relevant information necessary to identify the seller, as well as data related to past sales of goods using the rights-holders' trademarks and copyrights. Such disclosures would not only reassure rights-holders that the platforms are committed to addressing the problems, but could also provide greater opportunities for collaborative enforcement.

Beyond this sort of direct collaboration between platforms and rights-holders, IACC members have been supportive of increased information exchange among and collaboration between platforms and law enforcement to carry online investigations and enforcement actions into the real world to uncover the warehousing and manufacturing operations that supply online sellers. E-commerce platforms are only one part of the equation though. Rights-holders, law enforcement and customs agencies, financial service providers, internet registrars and registries, and shipping and logistics providers can each play key roles in abating the trafficking of counterfeit and pirated goods, and each of these stakeholders may have access to data that might assist the others in better identifying and rooting out those parties who seek to exploit legitimate business services to facilitate illegitimate ends. The ultimate goal of this collaboration should not be thought of only in terms of e-commerce platforms that are free

from counterfeit sales, but in terms of holistic improvements throughout the e-commerce landscape. To that end, the IACC has actively sought engagement with our partners in law enforcement, and with stakeholders across the spectrum of third-party intermediaries, as defined by the Presidential Memorandum.

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?**

IACC members consistently report that the overwhelming majority of counterfeit goods sold to U.S. consumers are sourced from China, and are either shipped directly to consumers from China, or from U.S.-based intermediaries who have previously purchased wholesale quantities from China/Hong Kong-based sellers. As a result, U.S. Customs & Border Protection is faced with a monumental task of targeting and interdicting those illicit shipments before they enter the U.S. market. CBP is a valued partner, its efforts consistently resulting in excess of 30,000 seizures annually, and accounting for over a billion dollars-worth of counterfeit goods – many of which are extremely dangerous – that would otherwise end up in the hands of U.S. consumers. There are, however, several issues relating to data sharing that if addressed, would make CBP's interdiction efforts more effective and help curb the flow of counterfeits sold online.

As noted above, and discussed in greater detail in the IACC's Written Statement for the Record to the Senate Finance Committee and other public filings, we strongly support full implementation of the authority provided to CBP by both Congress and the Administration in order to enhance both Customs' and rights-holders' abilities to address the trafficking of counterfeit and pirated goods. Such robust information sharing – both pre- and post-seizure – is consistent with the provisions set forth in and clarified by a number of actions including the enactment of the FY 2012 NDAA, TFTEA, and EO 13785. 19 CFR 133.21 should be amended to accurately reflect the full authority with which CBP has been imbued. Further, and in line with the direction included in Executive Order 13785, existing regulations should be clarified or amended as necessary to ensure that Customs personnel are empowered to share relevant data not currently enumerated in the regulations (e.g., information included on invoices, packing slips, bills of lading, including but not limited to order numbers and seller identification information connected to shipments facilitated by e-commerce platforms, delivery service tracking numbers, etc.). CBP's present interpretation of the Trade Secrets Act is seen as greatly diminishing the ability of rights-holders and Customs personnel to cooperate during the examination, detention, and seizure processes.

Regrettably, that interpretation of the Trade Secrets Act has also had an adverse impact on information sharing in the context of the agency's "Voluntary Abandonment" program. Originally developed as a pilot program, as part of an effort to increase the efficiency of IP enforcement in response to the drastic increase in express consignment shipments of counterfeit goods, the abandonment process enables CBP to circumvent the formal detention and seizure process by allowing importers / ultimate consignees to abandon a shipment suspected of containing counterfeit goods (and to permit expedited destruction of those goods). CBP has taken the position however that the regulations currently in place only permit the

disclosure of relevant import information to rights-holders in the context of formal detention or seizure; no such authority is provided in the regulations pertaining to abandoned shipments.

The lack of data is problematic, not only from an enforcement perspective, but from a business standpoint. Corporate brand protection teams rely upon interdiction data and other metrics to track the impact of their work and to justify the allocation of resources based in part on the efficiency and effectiveness of those resources in achieving results. Absent such data, the ability to carry out necessary analysis and to assess the effectiveness of brand protection efforts is greatly diminished.

In 2018, following its three-year pilot of the abandonment program, CBP confirmed its intention to roll out the program nationwide. According to some reports, approximately 12,000 shipments of suspected counterfeits had been abandoned in a one-year period. Over that same period, CBP seized a total of 34,000 counterfeit shipments; so voluntarily abandoned shipments appear to have accounted for over a quarter of all counterfeit shipments stopped at the border. Due to CBP's interpretation of the Trade Secrets Act, rights-holders have received no information regarding those abandoned shipments comparable to that provided in the case of formally-detained and -seized shipments. And while we believe that, properly implemented, a voluntary abandonment procedure could serve as an effective tool for mitigating the flow of counterfeits entering the market via small consignments; the decrease in actionable intelligence resulting from the program as it's currently operated is widely-viewed as a significant obstacle to rights-holders' own investigations. As CBP's IP enforcement activity has shifted more heavily to mail and express consignment shipments, rights-holders' concerns about the decreased availability of information related to illicit imports have grown more pronounced; some are already reporting an overall decrease in the number of seizure notices they've received in the past two years. Rights-holders' concerns in this area have been raised for several years, dating back to the operation of the pilot program; but we've seen little urgency to address these issues, despite direction from the Administration to do so, and despite reassurances that the concerns would be acted upon.

An adjacent concern to the above, involves CBP's delayed implementation of authority provided by Section 303 of the TFTEA to facilitate the sharing of relevant information related to its seizures of circumvention devices. For years, a legislative gap resulted in an absence of any clear authority for CBP to share information regarding such seizures with rights-holders impacted by the illegal importation of circumvention devices. That oversight was addressed by Congress with the enactment of TFTEA three years ago, but to date no regulations have been promulgated to implement the new statutory provisions. Given the normal distribution channels for circumvention devices though – they're typically purchased online and shipped directly to an end-consumer via small consignments – implementation of the TFTEA authority may result in little practical improvement in the availability of information to the relevant parties without also addressing the disclosure concerns related to voluntary abandonment.

While the existing regulations appear to permit CBP's disclosures post-seizure only to impacted rights-holders, we would welcome the provision of additional authority (or alternatively, sufficient clarification and guidance) to ensure that CBP is empowered to share relevant information regarding its enforcement activities with other stakeholders in the e-commerce distribution chain, including e-commerce platforms and shipping intermediaries.

And although rights-holders support CBP's disclosure to relevant stakeholders following both the seizure and abandonment of shipments of counterfeit and pirated goods, we continue to hear concerns voiced in the context of those procedures adopted for disclosure prior to a formal seizure. As discussed in our response to question three, the procedure adopted by CBP following the enactment of the FY2012 NDAA served largely to subvert the will of Congress. As set forth in the amended regulation, CBP established a process under which the importer of the goods is given seven working days to provide evidence of the goods' authenticity. During that period, rights-holders are precluded from receiving certain relevant information, including unredacted images of the suspected counterfeit products and their packaging. Neither the NDAA provisions, nor the as yet unimplemented provisions included in Section 302 of the TFTEA, make any reference to desirability or necessity of the importer to be involved in the authentication process. We're also unaware of what guidance, if any, CBP has provided to its personnel to use in determining whether evidence offered by an importer is sufficient to permit entry, or how CBP personnel go about validating claims or documents offered by an importer as evidence. Further, we know from experience that supporting documents such as authorization letters and certificates of analysis can be forged just as readily as the goods at issue. And as rights-holders have repeatedly argued since the process was established, the rights-holder is undoubtedly the most qualified party to make an accurate and expeditious determination of the goods' authenticity. The current process serves only to delay, and potentially decrease the likelihood of a positive identification of a counterfeit shipment.

With respect to the practical implementation of existing authority to share information with relevant rights-holders, IACC members also continue to report their receipt (when they do receive them) of seizure notices that fail to disclose mandated data points such as the name and address of an importer or exporter. Further, rights-holders have highlighted significant delays in the provision of seizure notices; impacted brands often receive such notices months after a seizure has taken place, and well beyond the deadlines prescribed in current regulations. Absent timely notice of seizures, rights-holders may be precluded from any opportunity to request samples of seized goods for examination, or be deprived of opportunities to investigate the matter in an expeditious manner.

While seizures of mail shipments consistently hover at approximately 10,000 per year, a variety of indicators support rights-holders' belief that that number should be significantly higher. China-based sellers frequently (and openly) advertise EMS China and China Post as their primary mode of transport, and we're likewise aware that the volume of international mail shipments far outstrips the volume of express consignment shipments; yet seizures in the express carrier environment accounted for more than 30% more of the total seizures reported in FY2017. The most logical explanation for this disparity, in the view of rights-holders, is the level and quality of Advance Electronic Data collected by the express carriers in comparison to that seen in the mail environment. We are hopeful that the enactment of the STOP Act may alleviate some of these concerns, but doing so will require full implementation and enforcement of that law's provisions. The increased data that should be available to CBP under a fully-implemented STOP Act should be leveraged with an eye towards improving targeting in the IP enforcement context, in turn leading to greater seizures of counterfeits in the postal environment.

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?**

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?**

We respond to questions six and seven together, noting that third-party marketplaces and other intermediaries currently engage in a variety of activities, and have implemented a range of policies aimed at combating the trafficking of counterfeit and pirated goods. At the outset, rights-holders have a number of baseline expectations with regard to the operation of third-party marketplace sites. Among these are that the platform operators will not knowingly illegally use rights-holders' IP, including the sale or fulfilment of orders for goods embodying or bearing their copyrights and trademarks; or use their IP for purposes of advertising or drawing consumers into the platform. There is a further expectation that e-commerce platforms will use their best efforts to identify and remove offerings for products that violate IP owners' rights, and will promptly respond to rights-holders' notifications regarding claims of violations. And there is an expectation that platforms will operate transparently and in good faith in addressing violations of IP on their platforms.

We believe a holistic approach is essential to creating a truly effective online enforcement regime, and encourage the adoption of best practices including those discussed herein.

<u>Identification and Vetting of Sellers</u>

As previously discussed herein, and in our recent testimony to the House Judiciary Committee's Subcommittee on Intellectual Property, the Internet, and the Courts, improved efforts to verifiably confirm an individual's identity before a seller is authorized to conduct business on a platform would provide an effective safeguard against the infiltration of platforms by known bad-actors, while also serving to prevent recidivism and counterfeiters' migration to other platforms following their identification and removal from a platform for IP violations. The vetting of merchants may also play an important role in protecting innocent victims whose identities have been stolen by the counterfeiters. We've received some troubling reports regarding the use of stolen consumer information by sellers as a means of concealing their true identities.

Merchants in the brick-and-mortar context are subject to a variety of regulatory oversight mechanisms including relevant licensing and tax registration processes; comparable oversight in the online market would be welcome. In its enactment of TFTEA in 2016, Congress imposed

"Know Your Customer" obligations on customs brokers, recognizing the key role that those parties play as gate-keepers for the market; similar actions by marketplaces in e-commerce to verify a party's identity, physical address, a registered agent for service of process, and related business entity and licensing information would be welcome – if not for all sellers, then at minimum for those who are engaged in sales on a commercial scale. Importantly, seller verification should not be limited to the onboarding process; sellers should be subject to periodic re-verification at least semi-annually to ensure that all relevant information is accurate and up to date, and sellers who fail to respond or to provide appropriate documentation should have their commercial privileges suspended. Such procedures would be beneficial not only with respect to IP enforcement matters, but also with regard to other consumer complaints.

As discussed below, the verification of sellers' identities – including any connections between individual seller accounts operated by the same individuals or organizations – is closely tied to ensuring that remedial actions are meaningful and lasting.

Robust Enforcement Policies to Deter Recidivism

Historically, enforcement of IP rights on online marketplaces has followed a "notice and takedown" model. As previously discussed however, those takedowns have often been the beginning of a cycle of the sellers relisting of the same items, new notices by the same rights-holders, and further action required by the platform. And absent an effective onboarding / vetting process for sellers, even those who have been "permanently" removed from a marketplace often find little difficulty in resuming their operations under a new name, or continuing their sales unabated, because the seller already operates multiple accounts on the platform. On some online third-party marketplaces, IACC members have reported specific infringing sellers hundreds or even thousands of times to the platform and yet these merchants are still active and continuing to sell counterfeits. Other marketplaces have begun developing stricter rules, such as "three strikes" policies, but these restrictions have often proven fairly easy for sellers to evade since these bans are often limited to particular products, rather than applying more broadly.

Above all, penalties must provide a meaningful and lasting deterrence to sellers of counterfeit goods. Some rights-holders, noting the integral role that platforms and payment processors play in providing the payment infrastructure for sales in e-commerce, have suggested imposing monetary penalties against sellers in cases of confirmed offenses. Such penalties, and the commissions charged by platforms for counterfeit sales, could be ear-marked to fund additional anti-counterfeiting activities including consumer education campaigns directed at online shoppers. As noted previously, suspending or terminating sellers' authority to conduct business on the platform for IP violations should amount to more than a slap on the wrist, and should not be easily skirted by using an alternate account or creating a new one. Prior to any reinstatement of privileges, disciplined sellers should be required to undertake training regarding their legal responsibilities and the site's rules related to IP protection, and the sellers should be subject to heightened scrutiny regarding the sourcing of the products they're purporting to sell.

Stricter repeat infringer polices, particularly if these polices were bolstered with greater information sharing about sellers' identities and more robust vetting processes, could

significantly decrease counterfeit sales online.

Addressing Sales Within Highly-Counterfeited and High-Risk Product Categories

The 2018 GAO report underscored the very real threats posed to consumers from the trafficking of counterfeit goods in e-commerce. In some product categories in particularly, the proportion of knock-off versions of branded goods has reached significant levels. As a preliminary consideration, rights-holders have strongly supported platforms' adoption of rules that require sellers to demonstrate that any products offered for sale are genuine and compliant with applicable safety standards including regulations under current law (e.g., CPHSA regulations). In light of the safety concerns involved, some marketplaces have taken steps to completely prohibit the sale of goods in high-risk categories. Similar actions, including restricting or filtering search functionality on the site for products in certain highly-counterfeited categories have also been taken by some marketplaces. We agree that these are appropriate actions to take under some circumstances, and we were pleased to see in the Comment Request that the interagency is already considering this as a potential aspect of "best practices" guidance.

Publication and Sharing of Information Regarding Counterfeit Sales

As discussed throughout these comments, we view the sharing of relevant data as a cornerstone of effective enforcement. As noted in our response to question four, rights-holders would welcome the sharing of more comprehensive data regarding sellers of counterfeit and pirated goods identified either through platforms' pro-active efforts, or in response to rights-holders' complaints. Information related to such sellers' verified identities, any connected user accounts, relevant historical data regarding their sales volume and products offered to consumers, and any information concerning the seller's importation, warehousing, or other relevant commercial services used to facilitate those sales would be desirable.
Similarly, information on a given seller's history of IP-related violations of platform policies should be readily accessible to consumers to allow for informed purchasing decisions and to minimize the chance that they will be defrauded.

Expanded Bases for Takedowns

Online sellers typically do not stop selling counterfeits after a brand pursues enforcement action on a platform, but instead alter their listings to make them more difficult to remove. One common trick is to remove direct trademark use but continue to use marketing images (including digitally altered images) to show the product, and to describe it in a way that misleads consumers into believing they will be getting a genuine product or an equivalent product that will look and operate the same way. Some brands have seen success in addressing these strategies of counterfeiters by working with platforms to seek listing removals on the basis of design rights or other rights. Most major global online third-party marketplaces now

remove infringing listings based on design rights, with the notable exception of eBay.com in the US. Accepting design rights has proven an effective tool to combat sellers of infringing "knockoff" sales and as well as listings that have been altered to avoid removal.

Rights-holders have also noted challenges historically in pursuing actions against products that infringe their legitimate utility patent rights, and that are being offered for sale on e-commerce platforms. We have heard some positive reports regarding a patent-focused dispute resolution program recently introduced by Amazon, and are encouraged by the news. We'd also support platforms' adoption of clear policies to remove listings and penalize sellers for offering for sale items the importation of which would violate exclusion orders issued by the International Trade Commission.

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.**

The IACC has been a consistent advocate for voluntary collaboration within the private sector to address a number of the challenges discussed in these comments. Particularly given the pace at which the online market has changed over the past two decades, and continues to evolve, voluntary programs taken by responsible participants in the marketplace may offer greater agility in terms of addressing emerging problems and the ever-changing tactics adopted by those trafficking in counterfeit and pirated goods. That said, we also firmly believe that there is a significant role that the government can and should play to ensure that the online market remains healthy and vibrant for all of the participants, whether rights-holders, consumers, legitimate retailers, or the third-party intermediaries who make e-commerce possible in the first place. Our recommendations for such action are included below.

<u>Administrative / Regulatory</u>

Ensuring the provision of necessary resources for the investigation of IP crimes, the interdiction of illicit goods entering the country from abroad, and the prosecution of violators remains an essential task of the government. Included under this broad mandate is the need for modernized tools (including improved technology) at our nation's more than 300 ports of entry, dedicated personnel with the necessary expertise in intellectual property enforcement, and updated and streamlined processes that take into account the incredible volume of legitimate and illegitimate trade that our border enforcement agencies are tasked with processing, and the ways in which they're being imported.

While CBP's Voluntary Abandonment process was developed as a means of addressing those

challenges, it's regrettable that it was designed and implemented with minimal input from the rights-holder community, and that the concerns raised by IP owners regarding that expedited procedure have gone largely unheard over the past several years. The amendment of relevant regulations, as discussed herein, should be undertaken without further delay to ensure that CBP is able to share relevant information with rights-holders about counterfeit shipments, regardless of the procedure used to prevent those goods' entry into the domestic market. Similarly, CBP's authority to seek necessary assistance – without delay – from IP owners, in determining whether the importation of goods would violate U.S. law, should be clarified. Finally, the agency's authority to share all relevant data related to the import (or attempted import) of a counterfeit shipment should be interpreted broadly to include information and relevant third-parties, whether enumerated in the current regulations or otherwise.

We would similarly encourage the adoption of improved procedures to enforce patent rights (including design patents) at the border. This action could provide significant assistance in combating the trafficking of "generic" product that is imported prior to labeling / finishing at facilities within the U.S.

Increased scrutiny and investigation of large-scale warehousing operations throughout the United States that serve as storage and fulfilment centers for the distribution of counterfeit goods offered for sale online would also be welcome. We've received increasing numbers of reports in recent years indicating a substantial growth in the scope and scale of such operations, which serve as vital link between overseas sellers and domestic consumers.

Legislative

Rights-holders widely view the present legislative landscape for online enforcement to be out of date. The rules of the road that apply today have remained largely unchanged since the early days of e-commerce, and were developed at a time when Congress' primary concern was to avoid over-regulation of the nascent market – as exemplified by the numerous safe harbors and limitations on liability for third-party intermediaries. While that framework no doubt succeeded in fostering the rapid growth of e-commerce; the statutes enacted, and courts' subsequent rulings, have in the view of many disproportionately placed the burden of enforcement on IP owners. The actual knowledge standard applied in the Tiffany v. eBay case, for example, set the bar so high as to preclude liability in seemingly all but the most extreme cases. Perhaps more importantly though, it served to enshrine "notice and takedown" – a process viewed by nearly all parties as ineffectual – as the only practical requirement to avoid a finding of liability.

Despite the development of improved technologies for identifying and reporting illicit activity on e-commerce sites, the intervening years have clearly demonstrated that an enforcement regime based on notice and takedown is a losing struggle. Given the reports of continued and significant concerns related to sellers' recidivism, it's not difficult to understand why so many feel that the court in Tiffany got it wrong, and that at some point, repeated and clear-cut sales of counterfeit and pirated goods should create a presumption of knowledge on the part of those who are enabling the sales.

During consultations with rights-holders in the preparation of these comments, some suggested the imposition of financial penalties in response to confirmed sales of counterfeits, particularly in those instances where the seller (and/or the seller's assets) are beyond the jurisdictional reach of civil or criminal enforcement, or in those cases in which the platform itself served as the importer of record for the counterfeit goods sold to U.S. consumers. Additionally, some have expressed interest in the development of an approach comparable to that of the U.K.'s Proceeds of Crime Act, which might compel third-party intermediaries to disgorge any profits earned as a result of sales of counterfeit or pirated goods through their platform.

II. SUPPLEMENTAL COMMENTS – Relevant IACC Programs

The IACC was founded on the principle that the trafficking of counterfeit and pirated goods is a problem too large for any single company to handle alone. That line of thinking has guided our approach in building out enforcement programs to address online trafficking in particular throughout the past decade. We view collaboration with partners throughout the public and private sectors as essential to protecting the rights of IP owners, the safety of consumers, and the vitality of the online marketplace as a whole.

As highlighted throughout this submission, data has long served as the lifeblood of intellectual property enforcement. But too often, the data available to any of the relevant stakeholders in the online ecosystem is limited – sometimes the result of current statutory or regulatory frameworks, but often simply because of a lack of recognition of that data's enforcement value, or the absence of an appropriate framework to share that information with relevant parties. Facilitating the robust exchange of relevant information in the context of IP enforcement, among and between e-commerce platforms, relevant government agencies, rights-holders, and other key third parties should be a priority for the government.

Seven and a half years ago, the IACC launched its first large-scale program, seeking to leverage the data and expertise of rights-holders and the world's largest credit card, payment processing, and money transfer companies. The RogueBlock[2] program, provided a streamlined, simplified procedure to leverage rights-holders' intelligence to assist partners in the financial sector to identify and remove bad actors from their systems. Operating independently, such enforcement action was simply not feasible, but by bringing those parties together, we've been able to identify and terminate thousands of merchant accounts used to service vast networks of rogue sites. This cooperative approach has continued to pay dividends as we've grown to become trusted partners, leading to expanded engagement far beyond the initial scope of our program.

In 2014, the IACC sought to apply a similar approach in the context of e-commerce platforms with the launch of the IACC MarketSafe Program[3]. That program, developed in partnership

[2] http://www.iacc.org/online-initiatives/rogueblock

[3] http://www.iacc.org/online-initiatives/marketsafe

with the Alibaba Group, established an enhanced framework for reporting and remediating infringing offerings on various Alibaba platforms, and to provide timely and relevant data regarding counterfeiters' evolving tactics and advice on policy- and procedure-based approaches to address those issues. Here, data again was a key component in that it served to guide the crafting of broad-based solutions that could be applied platform-wide. A similar approach has guided our more recent engagement with Amazon, as we seek to leverage data from program participants' experiences on the platform; specifically those where their initial complaints did not result in a satisfactory outcome. Our ultimate goal is to use this feedback to identify structural and procedural gaps that could be remedied to benefit rights-holders platform-wide.

The standalone websites, payment channels, and e-commerce platforms addressed by these programs though represent only a few of the opportunities that we believe are ripe for collaboration in the online realm. For approximately two years, we've been working to map out what a true industry-wide information sharing and collaborative enforcement program would look like in practice. That project, informally referred to as DataForce, seeks to engage a significantly broader range of e-commerce stakeholders, to include shipping intermediaries, internet registrars and registries, government, and other partners, in addition to those with whom we've historically engaged. To that end, we're actively working with the National IPR Coordination Center to reach out to such third-parties to discuss the development of appropriate mechanisms to enable the sharing of relevant enforcement information that may aid others in the space with regard to the identification and remediation of bad actors, with the ultimate goal of disrupting, dismantling, and demonetizing illicit criminal networks. This work remains ongoing, but to date we've had positive and productive discussions with these stakeholders.

The IACC has long taken the position that a safe and trusted e-commerce system is beneficial to all of the legitimate stakeholders who comprise it, whether rights-holders, legitimate retailers, service providers, or consumers; and that the robust enforcement of IP rights online is an essential component to ensuring a healthy online marketplace. Exchanging information with relevant partners is one way in which the responsibility can truly be shared.

We welcome the opportunity to work with partners in the public and private sector to build upon these ideas and put them into practice. And while we are cognizant of the fact that such an approach will require the application of substantial resources and effort from a range of stakeholders, we believe it provides a model for moving forward.

III. PRIOR RELEVANT SUBMISSIONS

As recognized by the Department's Request for Comments, rights-holders have been engaging with the Administration, past Administrations, and Congress on a range of issues relevant to the current inquiry for several years. To that end, we wish to highlight a number of pasts submissions that may provide additional context to our present submission and the interagency team's ongoing work in preparing the report described in the April 3rd Presidential Memorandum. These additional filings include:

- Comments in Response to USTR's 2018 Out of Cycle Review of Notorious Markets, available at: https://www.regulations.gov/document?D=USTR-2018-0027-0017
- Comments in Response to USTR's 2019 Special 301 Review, available at:

https://www.regulations.gov/document?D=USTR-2018-0037-0019

- Comments in Support of the IPEC'S 2016 Joint Strategic Plan, available at: https://www.regulations.gov/document?D=OMB-2015-0003-0048
- Comments in Support of the IPEC's Joint Strategic Plan for FY2020-2022, available at: https://www.regulations.gov/document?D=OMB-2018-0009-0028
- Written Testimony to the House Judiciary Committee, Subcommittee on Courts, Intellectual Property and the Internet, "Counterfeits and Cluttering: Emerging Threats to the Integrity of the Trademark System and the Impact on American Consumers and Businesses," July 18, 2019, available at: https://docs.house.gov/meetings/JU/JU03/20190718/109812/HHRG-116-JU03-Wstate-BarchiesiR-20190718.pdf
- Statement for the Record to Senate Finance Committee, "Protecting E-Commerce Consumers from Counterfeits," March 6, 2018, available at: https://www.finance.senate.gov/imo/media/doc/35965.pdf
- Statement for the Record to Senate Finance Committee, "Challenges and Opportunities for U.S. Businesses in the Digital Age," June 15, 2016, available at: https://www.finance.senate.gov/imo/media/doc/262471.pdf

We applaud the Department and all of our public-sector partners on the interagency team for their efforts on these important issues. We stand ready to provide any additional assistance or clarification that you deem necessary, and are available at your convenience.

Respectfully submitted,

Travis D. Johnson
Vice President – Legislative Affairs, Sr. Counsel