Hearing on "Counterfeits and Cluttering: Emerging Threats to the Integrity of the Trademark System and the Impact on American Consumers and Businesses"

Questions for the Record
Rep. Henry C. "Hank" Johnson, Jr., Chairman

Robert Barchiesi, President, International AntiCounterfeiting Coalition:

l. How can e-commerce platforms best keep pace with counterfeiters' changing tactics? Are there enforcement measures that e-commerce platforms can adopt that do not run the risk of being outdated or of being outmaneuvered?

To keep pace with counterfeiters, online platforms must responsibly devote resources to develop comprehensive programs to protect intellectual property rights (IPR). While there can be different operational approaches to IPR enforcement by online platforms, in our experience no single tactic, and no party working alone, can be successful. Comprehensive programs can generally be broken down into four core areas: (i) Notice and Takedown, (ii) Proactive Monitoring, (iii) Offline Enforcement and (iv) Stakeholder Collaboration, which has resulted in marked success and industry-best practices. Collaboration is among the most critical pieces – this isn't a problem that online platforms or rightsholders can or should solve alone.

Over the past decade, I've seen firsthand that the single most critical action that e-commerce platforms, and other intermediaries, can take to mitigate the sale of counterfeit and pirated goods being sold online is to share assets, resources, and expertise with rights-holders. The IACC has been a leader in this regard, working collaboratively across industries, and we have seen tremendous success. For example, in 2010, the IACC working together with the White House, launched a groundbreaking program in collaboration with Visa, Mastercard, American Express, PayPal, Discover, MoneyGram and Western Union. This "Follow the Money" approach recognized payment intermediaries as a logical choke point for rights holders to target. Further, utilizing payment blockades has enabled rights-holders and law enforcement to reach online criminal enterprises that are hosted abroad. The unprecedented cooperation by the payment industry raises the bar to which other intermediaries should strive.

In 2012, building upon the successes of the IACC's collaborative strategy, we reached out to Alibaba. We saw that the Taobao marketplace was rife with counterfeits and Alibaba lacked an effective IPR enforcement strategy. However, I also saw a company where the leadership was totally committed to working collaboratively to rid their marketplace of counterfeits. In the past four years alone, Alibaba has so substantially enhanced their IPR protection program to the point that we, and many other stakeholders are comfortable in referring their IPR protection program as the gold standard within the e-commerce industry. Moreover, we fully agree with the statement of the full Committee's Ranking Member, Rep. Collins, that

"…Alibaba's anti-counterfeiting policies and programs are significantly more effective than any of their U.S. counterparts."

In 2018, the IACC extended our outreach and collaborative approach to Amazon. To date, we have coordinated on a streamlined system to provide real time feedback regarding rights-holders' experience with Amazon's reporting tools. Further, the same mechanism allows rights-holders to inform Amazon's automated brand protection tools so that they can continue to iterate in response to counterfeiters' changing tactics and marketplace trends. This collaboration remains in its nascent stages though, and we're cognizant of the fact that wholesale change is not possible overnight. And while we're encouraged by the progress that we've seen to date, we also recognize that significant work remains to be done. Continued, and expanded, efforts are necessary to fully address counterfeiters' attempts to exploit the marketplace.

The aforementioned collaborative programs we've developed provide proof of concept for our approach. In working together, we have had a front-row seat to the evolution of counterfeiters' tactics to avoid detection; and to be frank, every action we've taken has been probed for gaps, loopholes, or technological workarounds by counterfeiters. I fully expect that this will continue to be the case, because, simply put, the profits that counterfeiters stand to make from their illicit trafficking are too large to expect otherwise. So, rather than searching for policies and practices that avoid the risk of becoming outdated or that risk being outmaneuvered, perhaps the better question is how we can develop an enforcement regime that is itself capable of evolving alongside counterfeiters' tactics.

And while it's likely that anti-counterfeiting efforts will remain, to some extent, reactive; as discussed in my earlier testimony, perhaps the greatest opportunity for improved enforcement can be found in proactive efforts to keep counterfeiters off of e-commerce platforms in the first place. We believe that there are a number of steps that could be taken to ensure that individuals seeking to sell to consumers – particularly those engaged in or intending to engage in commercial-scale activity, as determined by their volume of sales or advertised inventory – be held to a standard commensurate with that of their counterparts in the brick and mortar context. The development of industry-wide best practices for onboarding merchants, uniformly implemented, would serve to level the playing field to the benefit of all of the legitimate stakeholders. These should include requirements for obtaining and verifying a seller's name and address; relevant financial information; business documentation such as articles of incorporation, identification of officers, a registered agent, beneficial ownership, and licensing information, tax id numbers, and the like. Providing such documentation would be at most, a minimal inconvenience to legitimate sellers, and any such inconvenience would be easily offset in terms of the benefits realized by keeping counterfeiters from unfairly competing in the e-commerce market.

2. Are there any barriers or limitations that prevent e-commerce platforms from adopting technology-based mechanisms that address concerns regarding proper vetting and repeat offenders? What framework would best address those barriers and limitations, if so?

Counterfeiting operations have grown increasingly global in scale, and their supply and distribution chains far more complex. This inherently makes it more challenging for rights holders, law enforcement and online platforms alike. We view leveraging available technology as an important component of developing scalable solutions that can have a broad impact on IP enforcement efforts. In our attempts to do so however, we should not forget a term long-used by computer programmers, "GIGO" – "Garbage In, Garbage Out." If we're analyzing inaccurate, or incomplete, data, then even the most advanced technology will fail to provide the solutions we're seeking. Unfortunately, some of the greatest challenges we face with regard to leveraging technology more effectively are tied to our abilities to ensure that the information we have about sellers and the products they're offering for sale are accurate in the first instance, and to ensure that the information is available to those who are best positioned to make use of that data in the second.

As discussed above, obtaining verifiable information from prospective sellers – and, in fact, verifying the data provided – must be a threshold consideration. Congress has taken a similar approach with regard to the traditional distribution chain for counterfeit goods, with the enactment of Section 116 of the Trade Facilitation and Trade Enforcement Act, requiring customs brokers to adhere to minimum standards to confirm the identity of individuals seeking to make use of their services in bringing goods into the U.S. market. The same sort of commonsense logic should apply in the e-commerce context as well. A legitimate seller should be required to demonstrate proof of their identity, and those offering significant volumes of goods should likewise be required to demonstrate that they've sourced those products through legitimate channels. This would seem to be the bare minimum that consumers should expect in their interactions with online sellers or the platforms that facilitate those interactions.

Ensuring the accuracy of sellers' data at the time of onboarding (and periodically re-confirming its validity) is only one piece of the puzzle, however. Where illicit sellers have already infiltrated the system, and are later discovered to have been engaged in sales of counterfeit goods, that information should be made available to other platforms where the same individuals may have already established a presence, or to which they may seek to move their operations after a platform has taken action to block future sales of counterfeits. Such information sharing will aid in preventing counterfeiters from "forum shopping" for new outlets where they might go undetected. Similarly, where illicit sales have been positively identified on a given platform, information should be made available to other relevant stakeholders, including e.g., government partners such as U.S. Customs & Border Protection, who could leverage that data for improved targeting for the interdiction of counterfeit imports.

As noted in my oral testimony, we've begun exploring opportunities for such data sharing among e-commerce stakeholders across every sector. On the same day that the Subcommittee held this hearing, we participated in a working group meeting hosted at the National IPR

Coordination Center with numerous platforms and shipping companies. In that same vein, we've recently partnered with HSI to convene an IP Advisory Board consisting of representatives from 19 different industry sectors, financial and shipping logistics providers, e-commerce platforms, and our public-sector enforcement colleagues to provide a forum for discussion and collaboration on a range of voluntary efforts. The breadth of participants contributing to this effort, and the support offered by the relevant law enforcement agencies for this initiative is unprecedented; and I'm confident that it will facilitate concrete, practical action on these issues.

One of the avenues we're most interested in pursuing follows a model already in use within the financial sector to facilitate the sort of intelligence sharing discussed above to identify high-risk merchants with a demonstrated history of policy violations and/or illegal activity. To be clear, this is not a burden that can or should fall solely on the e-commerce platforms; rather, it demands a coordinated effort by all of the relevant stakeholders in both the private and public sectors. We've found great success and seen significant progress materialize from this sort of voluntary collaborative approach in the past, and will continue to seek greater engagement with a variety of stakeholders to achieve our ultimate goal of bringing about a truly safe and trusted online market.

Joseph Cammiso, President, Automotive Anti-Counterfeiting Council, Inc., Mr. Barchiesi, and Ms. Mond:

1. **Under the current system, rights owners typically bear the burden of policing individual marketplaces for counterfeits and submitting takedown complaints, which rights holders consider resource-intensive and ineffective at scale. What incentives could Congress provide to meaningfully change this system to one where e-commerce platforms play a larger role in proactively addressing the proliferation of counterfeit goods?**

As discussed in my prior testimony, we strongly support a more proactive approach to online enforcement against counterfeits. Generally speaking, rights-holders – and I expect most platforms too – would agree that the current notice and takedown process has proven to be extremely resource-intensive and fails to provide an effective means to curtailing counterfeit sales. The obligation of platforms to take action under current law is limited to those instances in which they have actual knowledge of the illegal activity. To that point, it is worth recognizing the investments and efforts that some platforms have made, which already go beyond those black-letter requirements. Proactive measures to screen sellers and listings, in some cases leveraging impressive data analysis and machine learning technologies, have obviated the need for direct intervention by rights-holders in many cases; but despite these efforts by e-commerce platforms, counterfeit sales online remain widespread. There is more that can and should be done to address the problem.

In my responses to the questions posed directly to me by Chairman Johnson, I highlighted the importance of improved collaboration and information sharing between stakeholders, particularly with regard to the vetting and onboarding of merchants. I firmly believe that the greatest opportunity we have to make a significant reduction in the volume of counterfeit trafficking online lies in keeping bad actors out of the system in the first place. It is the same logic applied in our government's broader IP enforcement strategy. While retail-level enforcement against individual sellers plays a role, the true "front-line" of enforcement is the border, where we seek to interdict illicit goods before they ever reach store shelves. In the same way, we should seek to keep counterfeit goods from reaching the virtual shelves of e-commerce platforms. U.S. Customs and Border Protection conducts targeting based on intelligence developed from its own past enforcement efforts, and the data generated by a broad range of actions undertaken by other stakeholders. Importantly, Congress has also imposed requirements that key parties, e.g., customs brokers, know their customers, and take necessary steps to verify relevant information about the individuals and entities with whom they're doing business. A similar approach to leverage stakeholders' data and expertise would be beneficial, and likely far less resource-intensive than the current notice and takedown paradigm, and we would welcome appropriate action by the Congress to facilitate such an approach.

2. Are there changes to the statutory standard for liability in counterfeiting cases that Congress should consider to effectively address the proliferation of counterfeit goods?

I do believe that Congress should continue to examine the statutory standard of liability (as interpreted by relevant case law). To be clear however, I view liability not as an end in itself, but as a mechanism for achieving the underlying goals of our IP protection and enforcement regime. As highlighted by Question 1 above, our current enforcement model is "resource-intensive and ineffective at scale;" the debate around liability arises, in turn, as a symptom of that dysfunction. In my written and oral testimony, I discussed at length the IACC's efforts in recent years to develop collaborative solutions that are both scalable and which equitably distribute the burden of enforcement among stakeholders. The progress that we've seen leads me to believe that the adoption of a more effective and proactive approach to enforcement online – keeping counterfeiters off of e-commerce platforms in the first place, preventing them from migrating their operations to other platforms or standalone websites, and imposing meaningful penalties when they have been identified – would to some extent obviate the need for considering broader liability.

I expect the Members of the Committee are well-versed in the current standard, arising out of the 2nd Circuit's ruling in the Tiffany v. eBay case. In brief, a platform operator cannot be held liable for sales of counterfeit goods on its platform by a third-party, unless the platform operator

has actual knowledge of the specific infringing activity at issue and fails to act expeditiously to remove or disable access to that listing. With its ruling, the court effectively enshrined a notice and takedown process that is widely viewed as an inefficient and ineffective means for dealing with the trafficking of counterfeit goods. A major concern has been that the court's ruling would serve as a ceiling on e-commerce platforms' efforts; as a practical matter though – at least in terms of the larger and more well-known platforms operating today – those concerns have not been borne out.

Though notice and takedown continues to play a significant role in the overall enforcement process, necessitating the investment of countless man-hours and financial expenditures; major platforms have worked both independently and in cooperation with rights-holders to develop proactive mechanisms that go far beyond the legal requirement of responding to takedown notices. These increasingly technology-driven solutions and practices adopted by those platforms are enabling more rapid identification and interdiction against bad actors. Those who have done so, including platforms that we're currently engaging with, should be recognized for those efforts. And if Congress chooses to re-visit the issue of where the line of liability should fall, some of these tools and practices that have been developed may offer insights into what is feasible, and what is reasonable. Further, Congress should not discount the potential impact of other tools to enable rights-holders and consumers to more effectively pursue counterfeiters (and their assets) located abroad, which would contribute to the same ultimate goal of ensuring that victims receive their just compensation.

I welcome the opportunity for further discussion of this issue, as well as Congressional support for the ongoing work within the private sector to identify and implement new tools and new approaches that will lead to a more efficient and more effective enforcement regime. As discussed in my testimony, I'm encouraged by the progress we've made in recent years, and with the continued engagement by stakeholders across the e-commerce ecosystem, as we seek to move beyond a notice and takedown model that has failed to keep pace with the practical realities of the online market.

3. What specific measures should e-commerce platforms use to better vet sellers and products? Is there a role Congress can play in assisting or incentivizing these efforts?

There seems to be widespread consensus among stakeholders that better vetting of sellers would significantly diminish the illicit trafficking of counterfeit goods online, and we are actively working to develop reasonable and effective criteria to provide a framework for such vetting. As a starting point, I would point to relatively recent work undertaken by U.S. Customs and Border Protection to implement Section 116 of the Trade Facilitation and Trade Enforcement Act – the so-called "Know Your Customer" provisions to be adopted by customs brokers in verifying and validating the identities of, and documentation provided by,

individuals and entities who seek to avail themselves of the brokers' services. Like customs brokers, e-commerce platforms are uniquely situated in the distribution chain to serve as a gate-keeper to identify bad actors before they're able to get their illicit wares to market.

Customs brokers are currently required by law to obtain a valid power of attorney from their clients, and the proposed rule published by CBP on August 14, 2019, provides a detailed discussion of the types of information that brokers are required to obtain from their customers, which include the following:

- The client's name;
- For a client who is an individual, the client's date of birth;
- For a client that is a partnership, corporation, or association, the grantor's [i.e., the individual executing the power of attorney] date of birth;
- For a client that is a partnership, corporation, or association, the client's trade or fictitious names;
- The address of the client's physical location (for a client that is a partnership, corporation, or association, the physical location would be the client's headquarters) and telephone number;
- The client's email address and business website;
- A copy of the grantor's unexpired government-issued photo identification;
- The client's Internal Revenue Service (IRS) number, Employer Identification Number (EIN), or Importer of Record (IOR) number;
- The client's publicly available business identification number (e.g., DUNS number, etc.);
- A recent credit report;
- A copy of the client's business registration and license with state authorities; and
- The grantor's authorization to execute power of attorney on behalf of client.

We believe the required data points provide an excellent starting point in terms of the sort of information that should be collected by e-commerce platform operators during the process of onboarding sellers. The Federal Register Notice detailing the proposed rule, likewise, provides guidance on how the required data points should be validated, including through the use of a variety of publicly available tools and databases. Importantly, the proposed rule requires this data collection and validation to take place *before* the broker begins conducting business on behalf of their customer; it also mandates periodic re-validation, and imposes recordkeeping obligations. Individuals or entities who wish to benefit from facilities offered by e-commerce platforms should be subject to similar requirements before they're permitted to sell to the public. While there may be some room for flexibility with regard to requirements imposed on casual sellers, the above should unquestionably apply to commercial sellers (i.e., those who exceed a certain level of sales or whose purported inventory exceeds a certain threshold). At minimum though, a sufficient level of detail must be applied across the board

to prevent sellers from operating duplicate accounts in an effort to skirt sales and inventory thresholds that might trigger the more stringent rules applied to commercial-level sellers.

As discussed previously, every seller on an e-commerce platform must, by necessity, link their account(s) to a payment account. Cooperation among platform operators and the financial sector to verify and validate information provided by sellers (and to better identify commonalities between seller accounts that may not be evident upon a superficial examination) could be extremely beneficial as well. We have found great success in our own work with the payment sector in identifying networks of related sites and sellers which could prove instructive in the platform environment as well. Communication among the variety of stakeholders is a high priority, and we'd also strongly encourage enhanced collaboration between individual platforms so that when high-risk sellers or bad actors have been identified and remedied on one site, they're not able to continue to act with impunity through other outlets.

One factor that is widely viewed as contributing to the persistence of illicit sales online is the lack of any centralized authority for the licensing of sellers as has long been the norm in the brick and mortar context. If I want to open a retail store here in Washington, there's a standard process for licensing and registration that I'm expected to follow. If I choose to open a new location in another state, I'm subject to that state's process as well. If I choose to open a virtual storefront though, I can sell to consumers in all 50 states and around the world with minimal oversight or regulation. I believe that to the extent possible though, the rules of the road should be the same for a seller whether they're operating online or off. There have been various proposals to fill that gap, including the development of a certification or similar process that could help to provide greater assurance of the legitimacy of online sellers, and we believe that such an approach warrants further exploration.

Counterfeiters should not be permitted to shield themselves from liability or from the scrutiny of consumers, legitimate online sellers, platforms, and rights-holders. By adopting reasonable, and dare I say commonsense, approaches to vetting sellers online; we can ensure that those sellers remain accountable for their actions.

4. What is a rights holder's recourse when a third-party counterfeit seller cannot be accurately identified, located, or served with a complaint? Who, if anyone, should be liable in these instances?

Rights-holders typically have fairly limited recourse when a third-party counterfeit seller cannot be accurately identified, located, or served with a complaint. Such difficulties have been a long-standing obstacle to effective enforcement online in the context of illicit sales through standalone websites; and there are countless examples of rights-holders litigating against John Doe defendants, or defendants who simply allow litigation to proceed in absentia,

confident in the fact that their assets are largely untouchable, and that any judgment obtained against them will be, in practice, unenforceable. While a multi-million dollar verdict in such a case may result in a catchy newspaper headline and draw some much-needed attention to the scope and scale of the problems faced by intellectual property owners, it does little in terms of providing any real monetary relief and any deterrence to future offenses is negligible. Further, given the costs associated with litigation, such cases are without a doubt a net loss for those plaintiffs. In the context of third-party sales on e-commerce platforms, any sort of financial recovery by rights-holders or consumers is likely to be exceedingly difficult where the seller of those goods cannot be identified, located, or served with a complaint. These types of difficulties are part of the reason that my testimony has stressed the vital importance of vetting sellers – not simply their identities, but also relevant business and financial information, information about their physical location, and their sourcing of goods. When bad actors are kept out of the marketplace in the first instance, liability ceases to be a concern.

With regard to the question of who, if anyone, should be liable for illicit sales by a third-party who cannot be located or identified, my thoughts largely mirror those expressed in response to Question 2, above. As set forth therein, current law does provide for platform liability in instances where the platform has actual knowledge of the items being counterfeit and fails to take reasonable action to prevent further sales; such liability would certainly be available even in cases where the seller could not be located. Absent factual circumstances that rise to meet the Tiffany v. eBay standard, we are aware of at least one recent case in another area of law which has raised the possibility of extending liability to a platform in cases where a third-party seller could not be located. The ultimate issue of liability in that case remains unsettled at this point, however.

Without some objective criteria which might be applied, it is a difficult task to make a blanket determination regarding to whom, or under what circumstances, liability should apply when a third-party seller cannot be located. If, for example, a platform has adopted and implemented reasonably robust procedures for vetting and onboarding merchants, and yet some bad actor has still managed to infiltrate the platform, and subsequently sells counterfeit goods to unwitting consumers, one might be hard-pressed to impose strict liability for those acts by third-parties. Conversely, where a platform operator has performed little or no due diligence with regard to the onboarding of third-party sellers, one must ask at what point does that sort of laissez faire approach rise to the level of actionable negligence or willful blindness. This is a question that remains unanswered by the current statutes, and the development of best practices in this area has been a priority in our ongoing discussion with other stakeholders.

As discussed previously, we view the extension of liability not as an end in itself, but as a mechanism for ensuring that injuries – whether the infringement of intellectual property rights or otherwise – can be compensated, and injured parties made whole. Other tools, for example – requiring third-party sellers to post a bond as surety to offset claims from rights-holders and

consumers – may also be available to accomplish that same goal. We would welcome the Committee's further investigation of this issue with an aim of identifying a range of potential remedies for pursuing third-party sellers and ensuring that appropriate remedies are available to victims even where those third parties remain out of reach.