Congress's Proposed E-Commerce Legislation for Regulation of Third-Party Sellers: Why It’s Needed and How Congress Should Make It Better

By John H. Zacharia and Kari Kammel

DRAFT
September 2020

Accepted for Publication with
U.C. Davis Business Law Journal
(forthcoming December 2020)

1 John H. Zacharia is the Founder of Zacharia Law PLLC, a law firm dedicated to helping victims of intellectual property crimes and cybercrimes protect their rights. He is also the former Assistant Deputy Chief for Litigation for the Computer Crime and Intellectual Property Section of the United States Department of Justice’s Criminal Division, where he became one of the most experienced federal prosecutors of intellectual property crime cases in the United States. Kari Kammel is the Assistant Director of Education and Outreach at the Center for Anti-Counterfeiting and Product Protection at Michigan State University and adjunct faculty at the Michigan State University College of Law.
When consumers buy items directly from brand owners online, consumers get exactly what they expect: the real item. Historically, when consumers bought online through an e-commerce platform, those same genuine items may also come directly from a brand owner or an authorized vendor. Today, however, third-party sellers have taken a larger share of the e-commerce retail pie. For example, more than half of Amazon.com’s [hereinafter “Amazon”] revenue now comes from third-party sellers. Although this shift to third-party sellers has significantly increased revenue for e-commerce platforms, it has also dramatically increased the number of counterfeit and defective goods sold on the most-visited e-commerce platforms – often with terrible consequences for consumers and brand owners alike. As a result, brand owners, consumers, and even the President of the

---


3 E.g., id. (“The business of selling other merchants’ goods is enormously lucrative for Amazon. In the last quarter, Amazon generated $18.2 billion of revenue from seller services such as fees and commissions, a figure that jumped 52 percent from the same period a year ago.”). As the Wall Street Journal observed, “[c]ompanies that profit from myriad small shipments have little financial incentive to stem the tide of counterfeit and pirated goods.” https://www.wsj.com/articles/u-s-signals-crackdown-on-counterfeit-goods-sold-online-11579820400.

4 As the New York Times noted, “the Government Accountability Office recently found that 20 of 47 items purchased from third-party sellers on popular consumer websites were counterfeit. Many of those products, which include car seats, airbags and baby formula, pose life-threatening risks.” https://www.nytimes.com/2020/03/02/us/politics/counterfeits-bill-china-amazon.html. In the same vein, the Wall Street Journal noted that the “size of the [counterfeiting] problem – and any likely solution – is growing. The incidence of infringing goods at U.S. borders has increased from 3,244 seizures in 2000 to 33,810 in 2018, according to DHS [Department of Homeland Security] data.” https://www.wsj.com/articles/u-s-signals-crackdown-on-counterfeit-goods-sold-online-11579820400.


6 For example, Birkenstock stopped selling its products on Amazon in 2016 because of “the proliferation of unauthorized sellers in the Amazon Marketplace, the possibility for counterfeit items and the brand’s inability to
United States continue to call on e-commerce platforms to do more to prevent third-party sellers from exploiting their platforms to sell counterfeit goods.

In this midst of these calls for action, Congress made a call of its own at the end of 2019 and in 2020. Congress proposed three different bills since December of 2019 – the Stop All Nefarious Toys in America Act (SANTA Act),\(^8\) the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-commerce Act of 2020 (SHOP SAFE Act of 2020),\(^9\) and the Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act (INFORM Consumers Act)\(^10\) – requiring e-commerce platforms to take preemptive steps to stop third-party sellers from selling counterfeit goods online. If passed, these bills would even create a cause of action against such platforms if they fail to act preemptively against third-party sellers of counterfeit goods. This article will (I) review the key events leading up to these bills, (II) analyze how each bill proposes to tackle the e-commerce counterfeiting problem, and (III) evaluate how Congress can improve the three proposed Acts and harmonize them into a more effective, single act of law.

I. Why Congress Proposed Bills Targeting Counterfeiting in E-Commerce


\(^7\) President’s Memorandum on Combating Trafficking in Counterfeit and Pirated Goods (April 3, 2019).

\(^8\) S.3073 — 116th Congress (2019-2020).


example, in June and July of 2020, compared with online sales in the prior year, e-commerce sales in the U.S. were up a respective 76% (June) and 55% (July).11

E-commerce provides the increased opportunity for businesses of all sizes to grow their business and brands globally and reach consumers that they would not with a traditional brick and mortar store, but with any technological advancement, what can be used for positive developments, also can be used by criminal elements. With the increase in e-commerce also comes the corresponding increase in the sale of counterfeit goods on these marketplaces. The Organization for Economic Cooperation and Development (OECD) describes the saturation of counterfeits in the market, jumping from $200 billion in 2005 to $509 billion in 2016.12 Further detailing this disturbing image in the U.S., the U.S. Department of Homeland Security (DHS) reported that seizures of infringing goods at US borders have increased tenfold between 2000 and 2018.13 In 2019, a U.S. Customs and Border Protection (CBP) operation found that almost 5% of all goods shipped from China and Hong Kong contained illicit and counterfeit products.14 E-commerce sites serve as the platform for many of these shipments, both business to consumer (B2C) and business to business (B2B).

Certainly, the problem of the online sale of counterfeit goods is as old as e-commerce itself. The shift by the largest e-commerce platforms to allow more third-party sellers has aggravated this problem by redirecting the trafficking of counterfeit goods into mainstream e-commerce. This increase in third-party sellers is both recent and dramatic. For example, in 2008, third-party sellers held a 30% share of the total paid units sold on Amazon15 – the world’s largest e-commerce

11 Stephanie Crets, Online sales taper off in July as retail stores reopen, DigitalCommerce360.com, Aug 11, 2020 (increasing sales 55% to $66.3 billion in July 2020 compared with July 2019, but a decrease from June to July, where in June 2020 online sales were up 76% year over year compared with June 2019), https://www.digitalcommerce360.com/2020/08/10/online-sales-taper-off-in-july-as-retail-stores-reopen/.

12 Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact (OECD 2016); see also Trends in Trade of Counterfeit and Pirated Goods (OECD 2019).


platform\textsuperscript{16} and most valuable retail company. By 2018, the share of total sales by third-party sellers on Amazon almost doubled to 58\%.\textsuperscript{17}

The shift by Amazon and other e-commerce platforms to selling the products of millions of third-party sellers instead of Amazon’s own products or authorized sellers of brand owners’ products\textsuperscript{18} comes with obvious economic benefits for the platforms. When third-party sellers use an e-commerce platform, the third-party seller selects which products it will sell, sources them from manufacturers or distributors, sets the purchase price, and uses the platform to reach consumers.\textsuperscript{19} If the e-commerce platform agrees to store the sellers’ products in the platform’s warehouses and ship them to the sellers’ customers,\textsuperscript{20} then the e-commerce platform does not incur the cost of buying the product. When third-parties use the e-commerce platform to sell their products directly to consumers\textsuperscript{21} \textit{(i.e., without asking the platform to store or ship the products)}, then the platforms do not incur

\textsuperscript{16} “It is the world’s most popular e-commerce website. In the United States, approximately half of all online shipping dollars are spent on Amazon.” Bolger \textit{v. Amazon.com, LLC}, 2020 WL 4692387, --- Cal. Rptr. 3d ---, at *2 (Cal. 4th Ct. of Appeals Aug. 13, 2020).

\textsuperscript{17} \url{https://finance.yahoo.com/news/amazon-third-circuit-third-party-liability-204536359.html}. Approximately 40\% of Amazon’s online sales were for products that “Amazon itself selects, buys from manufacturers or distributors, and sells to consumers at a price established by Amazon.” Bolger, 2020 WL 4692387, --- Cal. Rptr. 3d ---, at *2.

\textsuperscript{18} In a November 14, 2019 article, the Washington Post reported that, “in early 2018, Amazon began aggressively adding merchants, regardless of whether they were authorized by brands to sell their products.” \url{https://www.washingtonpost.com/technology/2019/11/14/how-amazons-quest-more-cheaper-products-has-resulted-flea-market-fakes/}.

\textsuperscript{19} E.g., Bolger, 2020 WL 4692387, --- Cal. Rptr. 3d ---, at *2.

\textsuperscript{20} Amazon’s “Fulfilled by Amazon” (“FBA”) program is one example of this arrangement. Under this program:

Third-party sellers must apply to register any product included in the FBA program, and Amazon may refuse registration for various reasons. . . . This service allowed [third-party sellers] to ship the products to Amazon’s warehouses; these products would be presented for sale within the Amazon.com Web site, and, if and when sold, would be shipped by Amazon to the buyer. Amazon may ship a product offered by one third-party seller together with products offered by other third-party sellers or by Amazon itself. Amazon controls the packaging for the shipment, which may include Amazon branding and Amazon-specific messaging.

To return an FBA product, the customer ships it back to Amazon, not the third-party seller. Amazon inspects the product and determines whether the product can be resold. If so, it will return it to the third-party seller’s inventory at the Amazon warehouse. If not, the third-party seller can have it sent back to its own facilities.

\textit{Id.} at *3 (internal quotations omitted).

\textsuperscript{21} E.g., Oberdorf \textit{v Amazon.com, Inc.}, 930 F.3d 136 (3d Cir.), vacated pending en banc decision (2019).
the costs of buying, storing or shipping third-party sellers’ products (or almost any other costs), as they would when selling their own products. In either case, e-commerce platforms collect the payment from the consumer for the third-party sellers’ products and then deduct a commission (a percentage of the sales price) and/or a fee (either on a per-item or monthly basis) from the third-party sellers.22 As a result, an e-commerce platform’s profit margin for allowing third-party sellers to sell their products on the platform is far greater than from the sale of the e-commerce platform’s own branded products.

By the same token, third-party sellers’ use of e-commerce platforms in this way comes with obvious risks to consumers. Unlike when it sells its own branded products, e-commerce platforms cede control to third-party sellers to decide which products to sell, the means of shipping those products, and even pricing. Thus, although e-commerce platforms will typically prohibit third-party sellers from trafficking in illegal products, a counterfeiter can easily circumvent this prohibition by making the counterfeit product appear genuine. Furthermore, e-commerce platforms may not collect sufficient information to identify third-party sellers – making it harder (and in some cases impossible) for customers or brand owners to pursue third-party counterfeiters or those selling counterfeits online. And when e-commerce platforms neither store nor ship the third-party sellers’ products, they are effectively choosing to be blindfolded from seeing whether the products sold by third parties are genuine, or even seeing third-party sellers’ real identities.

This shift can also be seen by e-commerce platforms that can also understand the risks that come with allowing third-party sellers onto their online marketplaces. For example, when Amazon made the decision to allow more third-party sellers on its platform to increase its revenues, the court in the recent Bolger v. Amazon case noted that Amazon correctly understood that there was a concomitant increase in

the risk that its platform would be used by third parties to sell counterfeit goods. In fact, for the first time in its history, in its February 1, 2019 Annual Report to investors, Amazon identified the sale of counterfeit, pirated, and other unlawful products on its platform as a risk factor. Specifically, Amazon stated that it: “may be unable to prevent sellers in our stores or through other stores from selling unlawful, counterfeit, pirated, or stolen goods, selling goods in an unlawful or unethical manner, violating the proprietary rights of others, or otherwise violating our policies.” Not only did Amazon acknowledge that third-party sellers could use its platform to sell counterfeit and other illicit goods, Amazon conceded that such sales “could harm our [Amazon’s] business or damage our reputation and we could face civil or criminal liability for unlawful activities by our [third-party] sellers.”

A. Some Federal and State Courts Begin to Impose Secondary Liability Upon E-commerce Platforms When Third Parties Use the Platforms to Sell Illicit Goods.

In 2019, the unlawful activity of third-party sellers became a liability reality for Amazon. On July 3, 2019, a Third Circuit panel applied Pennsylvania law to hold that an e-commerce business (in this case, Amazon) can be held strictly liable for a defective product sold on its platform by a third-party seller, even when the e-

---

23 Perhaps for this reason, some e-commerce platforms require consumers to accept this risk as a condition for using their platforms. For example, the California Court of Appeals in Bolger found in August 2020 that “Amazon’s consumer ‘Conditions of Use,’” state that

“Parties other than Amazon operate stores, provide services, or sell product lines through the Amazon Services. . . . We [Amazon] are not responsible for examining or evaluating, and we do not warrant the offerings of, any of these businesses or individuals or the content of their Web sites. Amazon does not assume any responsibility or liability for the actions, product, and content of all these and any other third parties.” The conditions go on to inform customers, in all capital letters, that “YOU EXPRESSLY AGREE THAT YOUR USE OF THE AMAZON SERVICES IS AT YOUR SOLE RISK.”

Bolger, 2020 WL 4692387, --- Cal. Rptr. 3d ---, at *4 n.2.


25 Amazon Added a First-Ever Warning about Counterfeit Product, see supra note 24.

26 Id.
commerce business neither possessed nor owned the defective product. In Oberdorf v Amazon.com, Inc., the plaintiff purchased a retractable dog leash from a third-party seller on Amazon. After taking the dog on a walk, the D-ring on the collar broke and caused the leash to retract into the plaintiff’s face – permanently blinding her in one eye.

When the plaintiff then sued Amazon for strict product liability and negligence in federal district court, Amazon initially prevailed on summary judgment because the court found that Amazon was not the “seller” of the defective product – it was a third-party seller, not Amazon, that chose to list the retractable leash on Amazon’s online marketplace and then ship it directly to the plaintiff. The district court found that Amazon’s role was limited to (1) listing the third-party sellers’ products on its “Amazon Marketplace,” (2) receiving order information from consumers, like the plaintiff, and (3) processing payments. Amazon merely collected the payment from the consumer and then deducted a commission (a percentage of the sales price) and a fee from the third-party seller.

On appeal, the federal Third Circuit panel vacated the district court’s ruling that Amazon could not be a “seller” for purposes of strict product liability. The panel held in Oberdorf that, where the third-party seller could not be located, the e-commerce platform could be deemed a seller if it exerted substantial control over third-party vendors. Moreover, Oberdorf held that Amazon had the ability to “exert[ ] substantial control over third-party vendors,” even though Amazon neither designs nor manufactures third-party products, in part through its enforcement of Amazon’s agreement with third-party sellers. Specifically, these agreements granted Amazon sole discretion to (1) prohibit or remove third-party sellers’ product listings; (2) withhold payments to third-party sellers; and (3) terminate

---


28 Id. at 140.

29 Id.

30 See id.

31 See id.

32 Id. at 146.
services to third-party sellers at any time. As a result, Oberdorf concluded that “Amazon is fully capable, in its sole discretion, of removing unsafe products from its website. Imposing strict liability upon Amazon would be an incentive to do so” and “will ensure that the company use[s its] relative position of power to eject [third-party] sellers who have been determined to be selling defective goods.”

Oberdorf further found that “Amazon is uniquely positioned to receive reports of defective products” and to remove such products from circulation because Amazon requires third-party vendors and consumers to communicate through Amazon – they cannot communicate directly. Despite this “unique position,” Amazon’s Vice President of Marketing Business “admitted that Amazon generally takes no precautions to ensure that third-party vendors are in good standing under the laws of the country in which their business is registered. In addition, Amazon had no vetting process in place to ensure, for example, that third-party vendors were amenable to legal process.” The panel concluded that Amazon “adheres to a business model that fails to prioritize consumer safety” because it enables third-party vendors “to structure and/or conceal themselves from the customer and from liability altogether.” “[H]ad there been an incentive for Amazon to keep track of its third-party vendors, it might have done so.”

On August 23, 2019, the Third Circuit agreed to rehear the Oberdorf case en banc, thereby vacating the panel decision. And on June 2, 2020, the Third Circuit certified the following question to the Pennsylvania Supreme Court: “Under Pennsylvania law, is an e-commerce business, like Amazon, strictly liable for a defective product that was purchased on its platform from a third-party vendor, which product was neither possessed nor owned by the e-commerce

33 Id.
34 Id. at 146, 147 n.35.
35 Id. at 145-46.
36 Id. at 145.
37 Id. at 145 & n.21, 146 n.28.
38 Id. at 147.
business?” The full Third Circuit’s decision is still pending as of the date of this publication.

Nonetheless, and pending that decision, the panel’s (now vacated) majority opinion in Oberdorf sent at least two important messages that immediately resonated with the public and with Congress. First, e-commerce platforms must be able to reliably identify and keep track of third-party sellers before they use the platforms to traffic in illicit products so the e-commerce platforms can use their unique position to stop such products before they reach consumers. Second, if e-commerce platforms choose to create a business model that limits (or, as in Oberdorf, precludes) consumers’ ability to communicate directly with third-party sellers, then those platforms will bear liability for the illicit products those sellers traffic using the platform.

Other recent strict liability cases against Amazon further highlight the increasing tension caused when consumers are unable to find third party sellers and whether the platforms themselves can be considered sellers. In State Farm Fire & Cas. Co. v. Amazon.com, Inc., a consumer who purchased a bathtub faucet adapter from a third party on Amazon’s website sued Amazon after the adapter malfunctioned and flooded plaintiff’s house. The federal court adjudicating the case still found that Amazon was a seller under Wisconsin law because “sellers and distributors are liable, not because of any particular activity on their part, but because they are proxies for the absent manufacturer. This structure suggests that, in the absence of the manufacturer, the entity responsible for getting the defective product into Wisconsin is liable.” This finding led the court to deny Amazon’s motion for summary judgment – and Amazon ultimately chose to settle the case.

Most recently, on August 13, 2020, a California state court of appeals reversed an e-commerce platform’s favorable summary judgment and held that California’s doctrine of strict products liability does apply to such platforms. In Bolger v.

---

42 Id. at 966.
43 Id. at 970.
Amazon, the plaintiff bought a replacement laptop battery from a third-party seller on Amazon’s online marketplace.\(^{45}\) The plaintiff, an Amazon Prime member, claimed that “the battery exploded several months later, and she suffered severe burns.”\(^{46}\) As a result, the plaintiff sued both Amazon and the third-party seller for, *inter alia*, strict products liability.\(^{47}\) In response, the third-party seller (though served) did not appear, and the trial court entered a default judgment.\(^{48}\) For its part, Amazon successfully moved for summary judgment in the trial court on the basis that it could not be held liable for strict products liability because Amazon successfully argued that it “did not distribute, manufacture, or sell the product in question.”\(^{49}\)

The California Court of Appeals reversed, and in the process made two significant findings as it relates to e-commerce platforms. *First*, and as the Third Circuit federal panel found in *Oberdorf* when applying Pennsylvania law, the panel in *Bolger* found that when an e-commerce platform merely “accepted an order for a product, billed the consumer, and remitted the proceeds to the upstream supplier,” California’s strict product liability rules could apply to the platform because it would still be “engaged in the business of selling” “as an intermediary between the upstream supplier and the ultimate consumer.”\(^{50}\) The fact that an intermediary does not manufacture, possess, or ship the product directly to the consumer does not allow the intermediary to categorically avoid liability under California’s strict product liability law.\(^{51}\) In addition, “‘neither the transfer of title to the goods nor a sale is required’ for strict liability to apply.”\(^{52}\) What *Bolger* did find relevant was the fact that Amazon controlled the transaction because, *inter alia*, it:

\(^{45}\) *Id.* at *1.

\(^{46}\) *Id.* at *1, *5.

\(^{47}\) *Id.* at *1.

\(^{48}\) *Id.* at *1, *5.

\(^{49}\) *Id.* at *1, *6.

\(^{50}\) *Id.* at *9* (citing *Canifax v. Hercules Powder Co.*, 46 Cal. Rptr. 552 (1965)) (internal quotations omitted).

\(^{51}\) See *id.* (citing *Canifax*).

\(^{52}\) *Id.* at *10* (quoting *Barth v. B.F. Goodrich Tire Co.*, 71 Cal. Rptr. 306 (1968)).
“created the environment (its website) that allowed [the third-party seller] to offer the replacement battery for sale;”

(2) “attracted customers through its own activities, including . . . its Amazon Prime membership program;”

(3) “set the terms of [the third-party seller’s] involvement, it demanded fees in exchange for [the third-party seller’s] participation;” and

(4) “required [the third-party seller] to indemnify it.”

Second, the California Court of Appeals found that applying California’s strict product liability rules to Amazon was easier in Bolger because, unlike in cases like Oberdorf, Amazon actually took possession of, and delivered, the product to the consumer. Specifically, “Amazon charged [the plaintiff] for the purchase, retrieved the laptop battery from its location in an Amazon warehouse, prepared the battery for shipment in Amazon-branded packaging, and sent it to [the plaintiff].” Unlike in Oberdorf, Amazon actually “took possession of the product, so it fulfilled the consumer’s order directly.” Amazon also “created the format for [the third-party’s offer for sale and allowed [the third-party seller] to use a fictitious name in its product listing.” In these ways, the Court emphasized that Amazon is a direct link in the chain of distribution, acting as a powerful intermediary between the third-party seller and the consumer. Amazon is the only member of the enterprise reasonably available to an injured consumer in some cases, it plays a substantial part in ensuring the products listed on its website are safe, it can and does exert pressure on upstream distributors . . . to enhance safety, and it has the ability to adjust the cost of liability between itself and its third-party sellers.

53 Id. at 11, *14.
54 Id. at *1.
55 Id. at *9, *11.
56 Id. at *11. Bolger also found that, “[e]ven setting aside the use of a fictitious name, the listing does not conspicuously inform the consumer of the identity of the third-party seller or the nature of amazon’s relationship to the sale.” Id.
As a result, the California Court of Appeals held that “Amazon should be held liable if a product sold through its website turns out to be defective.”

Courts have not been consistent in extending liability to e-commerce platforms for third-party sales. This is in part due to the fact that strict liability is handled at the state court level and is being brought by consumers, or a representative of consumers, who have been injured or killed. However, even where e-commerce platforms prevail in court, the cases continue to highlight the health and safety threat created by third-party sellers’ activities on e-commerce platforms. For example, in Stiner v. Amazon, parents of a teenager who died after consuming caffeine/protein powder purchased from a third-party seller on Amazon brought a strict liability suit under the theory that Amazon was the supplier. The Ohio state court found, among other things, that Amazon was not liable as a supplier of the lethal powder under Ohio’s strict liability law because Amazon lacked sufficient control over the caffeine powder.

Similarly, in State Farm Fire & Cas. Co. v. Amazon.com, Inc., a homeowner’s insurer brought a strict liability suit against Amazon after batteries in hoverboards purchased by the homeowners (from third-party sellers on Amazon) burst into flames that “caused severe damage” to the house. A federal court in Arizona granted Amazon’s motion for summary judgment because it found that, under Arizona law, Amazon “exercises insufficient control over such products.” Thus, even where Amazon has prevailed, these cases serve to underscore the health and

57 Id. at *2, *11-*12. The Court also held that Amazon could not rely on 47 U.S.C. § 230 (which, inter alia, precludes courts from imposing liability on service providers as speakers or publishers of third-party content) as a defense to the plaintiff’s strict product liability claims because the plaintiff’s “strict liability claims depend on Amazon’s own activities, not its status as a speaker or publisher of content provided by [the third-party seller] for its product listing. Id. at *2, *20.


60 Id. at 891-92.
61 Id. at 891.
63 Id. at 849.
64 Id. at 854-55.
safety risks consumers take when they buy certain products from third parties on e-commerce platforms.

As the above cases show, this shift to permitting more third-party sellers in the e-commerce space has not been adequately anticipated in the law—hence the need for new legislation. Because this shift toward third-party sellers does not fit neatly into existing secondary liability for trademark counterfeiting or strict products’ liability—we see the mixed results of consumers’ attempts to use both of those frameworks to address what seems to be an imbalance of responsibility and liability.

B. Public and Political Pressure Increases on E-commerce Platforms to Take More Proactive Measures to Stop Third-Party Sellers from Using E-commerce Platforms to Sell Illicit Goods.

As a result of these cases, and Oberdorf in particular, public pressure for e-commerce platforms generally (and for Amazon in particular) to do more to stop third parties from using their platforms to sell counterfeits only increased. One does not have to look far to see evidence of this greater public scrutiny.

On April 3, 2019, President Donald Trump issues Presidential Memo on Combating Trafficking in Counterfeit and Pirated Goods, which addressed the dangers and effects of counterfeit goods, with a specific emphasis on those that are imported through online third-party marketplaces and other third-party intermediaries and requesting a report from the Department of Homeland Security.65

On August 23, 2019, the Wall Street Journal published an article concluding (as did the Oberdorf panel) that “Amazon has proven unable or unwilling to effectively police third-party sellers on its site.”66 On November 14, 2019, the Washington Post (which is owned by Amazon CEO Jeff Bezos) wrote an article entitled “How Amazon’s Quest for More, Cheaper Products Has Resulted in a Flea


Market of Fakes,” in which the authors concluded that “Amazon’s system is failing to stanch the flow of dubious goods even with obvious examples of knockoffs.”67 And on January 14, 2020, a CNN report68 described how the infiltration of counterfeits in Amazon’s Marketplaces jeopardized the safety of children’s products such as car seats, swaddling blankets, and toys sold by counterfeitors, which was later highlighted by National Public Radio (NPR).69

Against this backdrop and in response to the April 2019 Presidential Memo,70 the U.S. Department of Homeland Security (DHS) issued a report on January 24, 2020 to the President of the United States entitled “Combating Trafficking in Counterfeit and Pirated Goods” that devoted an entire chapter to “How E-Commerce Facilitates Counterfeit Trafficking.”71 In that chapter, DHS bluntly criticizes the same e-commerce business model found wanting in Oberdorf:

Certain e-commerce platforms have adopted a business model that relies on North American warehouses to provide space for foreign-made goods, followed by one-at-a-time order fulfillment, at which point the goods are individually packed and shipped to U.S. consumers on much shorter delivery timelines. The platforms that use this model may also coordinate with customs brokers, as well as provide third-party logistics and freight forwarding services to assist with the initial delivery of goods to the warehouse.

Although this model is a significant innovation for legitimate commerce and provides benefits to consumers in the form of reduced costs and shipping time, it creates a mechanism that allows counterfeit traffickers to minimize transportation costs as well, while intermingling harmful


70 See supra note 66.

goods among legitimate goods. From a risk perspective, this model allows goods to enter the United States in a decentralized manner, allowing a counterfeit trafficker to spread the risk of seizure across a number of low-value packages. In situations where the fulfillment center is outside the U.S. Customs area, this model provides the opportunity to use ocean container shipping as the primary mode of transit for the shipment, which keeps overall shipping costs relatively low as ocean cargo is much cheaper than air delivery. It is in part because of these incentives that these fulfillment centers have emerged as an important element of the supply chains for many counterfeit traffickers.72

The DHS Report also made a series of recommendations to limit the trafficking of counterfeit goods in e-commerce, including two important ones. First, DHS recommended that the U.S. Government consider “pursu[ing] changes in the application of the contributory and/or vicarious infringement standards to [online] platforms” because “[o]nline platforms have avoided civil liability for contributory trademark infringement in several cases.”73 In essence, DHS recommends that the U.S. Government explore ways to impose secondary liability against e-commerce platforms to motivate them to adopt business models that better deter third parties from using these platforms to sell counterfeit goods – a goal that Oberdorf also championed.

Second, DHS recommended that e-commerce platforms significantly enhance the vetting of third-party sellers by requiring, “at a minimum,” the following:

(1) sufficient identification of the seller, its accounts and listings, and its business locations prior to allowing the seller to list products on the platform;

(2) certification from the seller as to whether it, or related persons, have been banned or removed from any major e-commerce platforms, or otherwise implicated in selling counterfeit or pirated products online; and

72 Id. at 24.
73 Id. at 33.
(3) acknowledgment, where applicable, that the seller is offering trademarked products for which the seller does not own the rights (either because they are a reseller or seller of used products).\textsuperscript{74}

In the same vein, DHS also recommended that e-commerce platforms increase transparency to consumers and brand owners by making the identity of third-party sellers and their country of origin available to the public \textit{before} a sale takes place.\textsuperscript{75} By both collecting (through enhanced vetting) and sharing this information, the platform will allow consumers to make more informed decisions before buying a third-party seller’s product, and it allows brand owners to identify unauthorized third-party sellers more quickly.

One week after the DHS Report, the President of the United States issued an Executive Order of his own related to counterfeit trafficking in e-commerce entitled “Ensuring Safe & Lawful E-Commerce for US Consumers, Businesses, Government Supply Chains, and Intellectual Property Rights.”\textsuperscript{76} In the Executive Order, the President stated that “[i]t is the policy of the United States Government to protect consumers, intellectual property rights holders, businesses, and workers from counterfeit goods . . . now being introduced into the United States as a result of the recent growth in e-commerce.” He further stated that “e-commerce platform operators[] should not facilitate importation involving persons who are suspended or debarred by” U.S. Customs and Border Protection (CBP), strongly suggesting that e-commerce platforms must do sufficient vetting of third-party sellers to identify and to preclude those sellers that CBP has already suspended or debarred.

\textbf{C. How E-commerce Platforms Have Reacted.}

Finally, before discussing Congress’ proposed legislation, we will note how e-commerce platforms have reacted to increasing pressure to stop third-party sellers from using their platforms to sell illicit or counterfeit goods with new efforts.

\textsuperscript{74} \textit{Id.} at 35-36.

\textsuperscript{75} \textit{Id.} at 38-39.

Although e-commerce platforms have announced new efforts to combat counterfeiting, the effectiveness of these new efforts is not yet clear. Alibaba was one of the first e-commerce platforms to require China-based third-party sellers to provide their National Identity Cards before they could advertise their products on the platform and has since continuously increased its sophistication in verifying sellers to avoid seller identity fraud or deception.\(^{77}\)

For its part, Amazon made a series of new announcements in its efforts to combat counterfeits sold on its platform. For instance, on January 13, 2020, and perhaps in anticipation of the DHS Report’s release less than two weeks later, Amazon announced though an anonymous source that, going forward, it “will report a merchant’s name, company name, product and contact information to authorities, after it confirms a business was selling fakes, closes the seller’s account, and the account holder does not make a successful appeal via Amazon’s typical processes.”\(^{78}\) This effort may produce an impressive number of referrals to law enforcement, but it may not be a good measure of its effectiveness for one simple reason: evidence of counterfeiting alone is not a federal crime. Federal law generally authorizes criminal prosecutions only against those who intentionally traffic in goods and knowingly use a counterfeit mark.\(^{79}\) Recent initiatives with the National Intellectual Property Rights Coordination Center, part of the U.S. Department of Homeland Security, have been coordinated to discuss data sharing

---

\(^{77}\) In 2003, when Taobao was established, Taobao required that the responsible person of a new store register with his/her real names. See generally, Taobao Terms of Services, https://www.taobao.com/helpcenter/content/help_rule_register_en.html. In 2005, Taobao further required that the bank records needed to be verified. In 2014, Alibaba started a new practice of requiring store owners to provide selfies of themselves with particular poses or certain objects, for the purpose of real-person certification of their ID documentation. Most recently, in 2015, Alibaba upgraded their system of using biotechnology for verification was further upgraded, including voice and even facial expression recognition. See e.g. Face++, Whose Facial Recognition Tech Is Used By Alibaba, Raises $25M — TechCrunch, Tech Crunch, May 15, 2015, https://techcrunch.com/2015/05/14/faceplusplus/.

\(^{78}\) “Amazon to Ramp Up Counterfeit Reporting to Law Enforcement,” Reuters, Jan. 13, 2020, https://www.reuters.com/article/us-amazon-com-counterfeit/amazon-to-ramp-up-counterfeit-reporting-to-law-enforcement-idUSKBN1ZC25U. As Reuters noted: “The move comes as Amazon faces public scrutiny over how it polices counterfeits and allegedly unsafe products on its platform. . . . Now, the company plans to disclose merchant information to European and U.S. federal authorities every time it confirms a counterfeit was sold to customers, increasing the frequency and volume of reporting to law enforcement, according to the person, who spoke on condition of anonymity. Why the new program was happening now was not immediately clear.” Id.

\(^{79}\) See generally 18 U.S.C. § 2320.
with federal law enforcement.\textsuperscript{80} However, flooding law enforcement with information about thousands of third-party sellers without any evidence that the seller knew the mark was counterfeit will probably be an empty exercise that will lead to few new federal criminal trademark counterfeiting prosecutions.

Amazon proposed another information-sharing initiative on April 2, 2020, when it announced that it had expanded its 2018 program with the International AntiCounterfeiting Coalition (IACC) by offering IACC member brands “insight into the counterfeit sales volumes of known infringers.”\textsuperscript{81} “The IACC and Amazon expect this expansion to help drive criminal referrals and litigation against bad actors holding them accountable for their illegal activities and protecting customers and rights owners.”\textsuperscript{82} This initiative may help IACC member brands better “target the most egregious counterfeiters,”\textsuperscript{83} which is helpful to brand owners who are also IACC members; but this expanded program does little to deter third-parties from listing counterfeits on Amazon’s platform in the first place.

On April 26, 2020, Amazon announced a more promising pilot program that involves using video conferencing to verify the identity of third-party sellers.\textsuperscript{84} Amazon began the notion of live verification of sellers’ identities using in-person meetings two months earlier, but shifted to video conferencing because of the Covid-19 crisis.\textsuperscript{85} Under this program, an Amazon associate compares a prospective third-party seller’s ID and the seller’s application documents with the seller participating in the video call to ensure that they match.\textsuperscript{86} Although it is too soon to evaluate how effective this proactive program will be, this pilot program may be Amazon’s most promising proposal to date because it has the potential to


\textsuperscript{82} Id.
\textsuperscript{83} Id.


\textsuperscript{85} See id.
\textsuperscript{86} See id.
weed out fraudsters and counterfeiters before the seller has the chance to list illicit goods on Amazon’s online marketplace.

In a further effort to combat counterfeiting, Amazon announced on June 24, 2020 that it was forming a “Counterfeit Crimes Unit” to combat counterfeit goods sold on its online marketplace. Although the name of the unit uses the word “crimes,” it appears that Amazon intends for this unit to support the efforts of members of law enforcement as they investigate criminal counterfeiting. Despite the name, Amazon announced that this new unit will also “enable[] Amazon to more effectively pursue civil litigation against bad actors.” Amazon has filed cases against counterfeiters in conjunction with brands since 2018. And Alibaba appeared to take the lead in the U.S., as that e-commerce platform had announced a similar effort at least as far back as 2017.

The deterrent effect of this civil litigation effort has two significant limitations. First, these cases will have little, if any, deterrent effect against third-party sellers who reside and operate overseas because they are usually outside the jurisdiction of U.S. federal courts and often do not even appear. To the extent that such overseas third-party sellers represent the bulk of third parties using e-commerce platforms to sell counterfeit goods, federal civil litigation will probably not target the very third-party sellers who need to be deterred the most. Second, although

---


88 In its press release, Amazon states that the unit will “aid law enforcement officials worldwide in criminal actions against counterfeiters.” Id.


91 As TheFashionLaw.com noted, Amazon’s new effort to join brand owners’ lawsuits “does not appear to be all that different from the robust campaign that Alibaba launched years ago to in order to shed perceptions that its websites were riddled with fakes – a key to gaining a bigger international customer base and taking market share from global competitors, such as eBay and Amazon.com.” https://www.thefashionlaw.com/amazon-files-another-joint-counterfeit-suit-this-time-with-kf-beauty/.

joining civil trademark counterfeiting suits are efforts that are easy to promote in a press release, they are reactive, after-the-fact efforts whose deterrent effect is equally easy to overstate. Brand owners are perfectly capable of filing civil trademark counterfeiting suits against online third-party sellers, and they have been doing so for years. However, brand owners’ civil suits alone have not proven sufficient to deter third-parties from selling counterfeits online, particularly those who are not based in the U.S., and e-commerce platforms joining these suits adds little, if any, additional deterrent value to brand owners’ existing efforts.

E-commerce platforms’ efforts should be proactive, directed toward identifying and targeting third-parties who attempt to use their platforms to sell counterfeit and illicit goods before the sellers have the chance to list such goods publicly on the platform. E-commerce platforms do have such programs already; however, as already noted, federal courts, state courts, and the federal government have weighed and measured those efforts and have found them wanting. Some e-commerce platforms have called for legislation to regulate how secondary liability should be imposed on them. For example, in the course of the Bolger v. Amazon litigation, Amazon called on California to enact legislation to clarify how California’s strict products liability law applies to e-commerce platforms. And to its credit, Amazon supported an effort by a California legislator to do just that.

E-commerce platforms should also support Congress’ efforts (discussed more fully below) to craft legislation targeting counterfeiting in e-commerce. Doing so

93 For example, Gucci has stated “that it spends ‘significant monetary resources’ to ward off counterfeiters” and that “[t]he exponential growth of counterfeiting over the Internet has created an environment that requires companies, such as Gucci, to file a large number of lawsuits.”


95 Bolger, 2020 WL 4692387, --- Cal. Rptr. 3d --- , at *16 & n.9.

96 “Burning Laptops and Flooded Homes: Courts Hold Amazon Liable for Faulty Products;” The Washington Post, Aug. 29, 2020, https://www.washingtonpost.com/technology/2020/08/29/amazon-product-liability-losses/; https://www.prnewswire.com/news-releases/survey-86-of-amazons-third-party-sellers-profitable-going-into-2020-301006354.html (“Bolger’s case and others in California led to a first-of-its-kind bill that would have extended rules that apply in the physical world to electronic commerce. The bill, which Democratic Assemblyman Mark Stone pulled late Friday as the legislative session neared its end, called for holding online marketplaces liable for the products they sell, just as retailers can be held responsible for goods purchased in their brick-and-mortar stores. . . . Amazon supported the measure, with one condition: the company wanted the law to apply to all online marketplaces”).
will not only help Congress understand all the ways in which e-commerce platforms can stop third-parties from selling counterfeit goods before such goods are listed on their respective platforms. It will also demonstrate to consumers, brand owners, and the federal government that e-commerce platforms are willing to change their business models to prioritize protecting consumers over making money from third-party sellers.

II. Congress’s Proposed Bills to Target Counterfeiting in E-Commerce

In the midst of, and as a result of, this cacophony of calls for action – from federal courts, the public, DHS, and even the President – to turn back the rising tide of counterfeits on e-commerce platforms, Congress proposed a series of bills attempting to do just that.

A. The SANTA Act

In December of 2019, Congress proposed the first of these bills – the Stopping All Nefarious Toys Act (“SANTA Act”). The momentum from this bill came from the toy industry and brands, and particularly some of their research on consumer purchasing of counterfeits online and specifically the challenge of finding the identify of third party sellers.

The SANTA Act came out of industry action, but also some recent cases that demonstrate the need for an increase in regulation of the sale of children’s toys on online marketplaces. In Spin Master Ltd. v. Alan Yuan’s Store, the U.S. District Court for the Southern District of New York held that a seller of a counterfeit hand-held fairy toy with moveable wings over an online marketplace platform was liable for trademark infringement under the Lanham Act as well as copyright infringement and unfair competition when there are no immediately noticeable differences between the counterfeit toy and the original, and when the seller uses the marks and copyrighted materials belonging to the plaintiff without permission.

---

97 S.3073 — 116th Congress (2019-2020)(introduced by Bill Cassidy (R-La); cosponsored by Senators Thom Tillis [R-NC], Robert Menendez [D-NJ], and Richard Durbin (D-IL).

or a license. The brand owner’s investigation prior to the suit found that counterfeit fairy toys bearing the “Flutterbye” marks being sold on e-commerce platforms Alibaba.com, Aliexpress.com, and DHgate.com. Although these platforms required the disclosure of minimal information from merchants regarding the identity of the seller, manufacturer, and distributor of the products, consumers were still confused. The court agreed with the brand owner and imposed a permanent injunction against the defendants, as well as statutory damages of $50,000 per defendant.

Prior to Spin Master, Rovio Entertainment Ltd. v. Royal Plush Toys, Inc. demonstrated how sellers of counterfeit toys often attempt to confuse the public into thinking the counterfeits are the originals. In Rovio, the District Court for the Northern District of California found a group of defendants responsible for the manufacturing and sale of counterfeit plush toys liable for trademark infringement, false destination of origin, passing off, and trademark counterfeiting.

The Toy Association, the industry group made up of toy brands, worked with Senators Cassidy, Tillis, and Menendez on the bill and testified before Congress about the impacts of counterfeits in the toy industry. The association had previously conducted research which showed 1 in 3 parents believe counterfeit goods are not sold on major online marketplaces and had created a guide for parents to help avoid counterfeit products. Additionally, the Toy Association published a whitepaper concerning counterfeit toys on e-commerce markets and

100 Id. at 419.
101 Id.
102 Id. at 426, 427.
104 Id.
made specific legislative proposals. The SANTA Act incorporates some of the Toy Associations’ recommendations.

The SANTA Act would require online marketplaces to make information of the identity of any seller of a new and unused children’s product by requiring the seller to provide information relevant to the sourcing, distribution, or manufacturing of products of third party sellers available to potential customers. The SANTA Act requests that online marketplaces conspicuously disclose the following information: verification of the seller through bank account information, photo identification, individual/business contact information, the seller’s name, contact information, and business address, and the location where the seller is the manufacturer, importer, or reseller. Additionally, there is a provision noting disclosure if the seller is not the fulfiller or shipper of the product. The bill is limited to children’s products intended for children 12 years and under. Additionally, enforcement of the SANTA Act is to be considered a violation of the unfair or deceptive practices act under the Federal Trade Commission Act.

Overall, the SANTA Act attempts to shift the burden from the IP rights holder, or the brand owner, to the e-commerce platform and the sellers since the lack of transparency of the sellers makes it challenging to pursue them for any type of legal action or even take down of infringing storefronts or illicit goods postings. Additionally, it seeks to empower consumers with the added transparency, particularly since consumers overall tend to be trusting of e-commerce platforms.

Moreover, this Act focuses on liability that the e-commerce platforms would have under the unfair trade or deceptive practices act. This seems to be limiting given the other case law surrounding these types of issues that have been occurring

109 Id. at Sec. 2 (a)-(b).
110 Id. at Sec. 2(c).
111 Id. at Sec.
112 Id. at Sec. 2(d) (noting that “A violation of subsection (a), (b), or (c) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))).}
on e-commerce platforms in the past ten years and accelerating with increased frequency. Further, it relies on a similar technique used by Chinese e-commerce platforms, reliance on national IDs and documents, but does not detail how stringent that verification process is. What can be learned from the Chinese experience is that the requirement of these items is not foolproof in deterring the sale of counterfeit goods, since these can easily be faked, stolen, or used in some other fraudulent way.

While the SANTA Act was championed by an industry that must take health and safety considerations seriously, it has shortfalls when coming to what it covers—for example, it is limited to children’s products for ages 12 and under. While the SANTA Act overall is an important step in the right direction, it would gain strength by joining in with other industries to have a much wider scope to any products sold online in this context and perhaps a broader chance for enforcement to incorporate either contributory trademark liability or strict liability into its language.

B. SHOP SAFE Act of 2020

On March 2, 2020, a bipartisan group of members of the House of Representatives proposed the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-commerce Act of 2020 (SHOP SAFE Act of 2020). The stated purpose of the bill is primarily “to provide for contributory liability for certain electronic commerce platforms for use of a counterfeit mark by a third party on such platforms.” This is a bipartisan bill seeking to impose accountability upon e-commerce platforms for counterfeit goods that threaten consumers’ health and safety. As one cosponsor of the bill, Representative Doug Collins (R-GA), stated when the bill was introduced, “[c]onsumer lives are at risk because of dangerous counterfeit products that are flooding the online marketplace. Congress must create accountability to prevent these hazardous items from

---

113 H.R. 6058 — 116th Congress (2019-2020) (introduced and cosponsored by Jerrold Nadler (D-CA), Doug Collins (R-GA), Hank Johnson (D-GA), and Martha Roby (R-AL).

114 Id. at Preamble.
infiltrating the homes of millions of Americans.”115 Fellow co-sponsor, Representative Jerrold Nadler (D-NY), added that

[I]t is clear more must be done to combat the rising trend in online sales of counterfeit products . . . Consumers should be able to trust that what they see and purchase online is what they will get, but counterfeiters continue to join platforms with ease and masquerade as reliable sellers in order to infect American households with dangerous and unsafe counterfeit products. The SHOP SAFE Act proposes a set of commonsense measures to tackle the gaps in these platforms’ systems and stop counterfeit sales.116

In the SHOP SAFE Act of 2020, Congress proposes to amend the Trademark Act (Section 1114 of Title 15 of the U.S. Code) by adding a provision imposing upon e-commerce platforms contributory liability “for infringement117 by a third party-party seller participating on the platform for use in commerce of a counterfeit mark in connection with the sale, offering for sale, distribution or advertising of goods that implicate health and safety.”118 However, the bill also creates a safe harbor for those e-commerce platforms that adopt business models complying with a series of requirements that, perhaps not coincidentally, also address many of the same concerns raised in Oberdorf.119

For example, the bill sets forth a number of provisions requiring e-commerce platforms to make it easier for consumers (and brand owners) to identify third-party sellers and to sue third-party counterfeiters for direct liability – an option that was unavailable to the plaintiff in Oberdorf. To qualify for the safe harbor, e-commerce platforms may only allow third-party sellers who are “available for service of process in the United States” to use its platform.120 Although this


116 Id.

117 The bill is not consistent in its use of the terms “counterfeit” and “infringement” – terms that have different meanings under the Lanham Act that this bill proposes to amend. If Congress’ goal is to impose contributory liability on e-commerce platforms when third-party sellers use a counterfeit mark on goods sold on these platforms, then it is important for Congress to ensure that it uses the term “counterfeit” consistently.

118 Id. at Sec. 4(A).

119 Id.

120 Id. at Sec. 4(A)(i).
requirement does not limit e-commerce platforms to U.S.-based third-party sellers, it does ensure that they must have a sufficient U.S. presence to be available for service of process. The bill also requires e-commerce platforms to take a series of steps\textsuperscript{121} to use “reliable documentation” (like governmental identification) to verify “the identity, principal place of business, and contact information” of every third-party seller using the platform and to “conspicuously” display such information on the platform.\textsuperscript{122}

To further facilitate pursuing third-party sellers directly liable for trademark counterfeiting, the bill states that e-commerce platforms must also require third-party sellers to consent to federal jurisdiction “with respect to claims related to the third-party seller’s participation on the platform.”\textsuperscript{123} And if third-party sellers use counterfeit marks on goods listed or sold on the platform, then platforms must provide the identifying information to law enforcement and, upon request, to brand owners.\textsuperscript{124}

In addition to imposing requirements making it easier for brand owners, consumers, and law enforcement to pursue third-party sellers who commit trademark counterfeiting, the SHOP SAFE Act of 2020 requires e-commerce platforms to take both proactive and reactive measures to facilitate taking down counterfeit goods that pose a threat to health and safety and to remove third-parties who offer to sell such goods on the platforms. Specifically, platforms must implement “proactive technological measures” that screen third-party sellers’ goods \textit{before} displaying the goods to the public to prevent sellers from using a counterfeit mark in a listing or sale on the platform.\textsuperscript{125} E-commerce platforms must also “expeditiously disable or remove from the platform a listing by any

\textsuperscript{121} The proposed bill currently fails to expressly indicate whether the requirement set forth in what would be subsection 1114(4)(A)(i) and those set forth in what would be subsection 1114(4)(A)(ii) are cumulative (by using the word “and”) or in the alternative (by using the word “or”). This appears to be a scrivener’s error, as it is clear from the language in § (4)(A) that immediately precedes subparagraphs (4)(A)(i) and (4)(A)(ii) that Congress intended these requirements to be cumulative, not in the alternative. To eliminate any ambiguity, Congress should simply insert the word “and” between subparagraphs (4)(A)(i) and (4)(A)(ii).


\textsuperscript{123} \textit{Id.} at Sec. 4(A)(ii)(III)(bb).

\textsuperscript{124} \textit{Id.} at Sec. 4(A)(ii)(X).

\textsuperscript{125} \textit{Id.} at Sec. 4(A)(ii)(VI).
third-party seller that reasonably could be determined to have used a counterfeit mark” and preclude “any third-party seller that has engaged in more than three instances of use of a counterfeit mark” from using (or rejoining) the platform.126

To qualify for the safe harbor, the SHOP SAFE Act of 2020 also requires e-commerce platforms to take due diligence steps of their own to ensure that third-party sellers neither list nor sell harmful goods on the platforms – another goal of the Oberdorf panel. For instance, the bill states that platforms must require third-party sellers “to verify and attest to the authenticity of goods” that they sell bearing registered marks and agree not to use counterfeit marks on goods sold on the platform.127 E-commerce platforms must also require third-party sellers to use only those images that the seller either owns (or has permission to use) and that “accurately depict the actual goods offered for sale on the platform.”128

Most significant, the SHOP SAFE Act of 2020 requires e-commerce platforms to take these verification and due diligence steps “[b]efore any alleged infringing act by the third-party seller”129 if they want to take advantage of the bill’s safe harbor. In other words, it is not enough for e-commerce platforms to adopt business models that purport to combat counterfeiting after-the-fact – such as filing or joining a civil counterfeiting or trademark infringement case after the infringing product is listed or sold on the platforms. If the platforms wish to avoid contributory liability under this bill, then they have to use their leverage over third-party sellers (as Oberdorf noted) before harmful counterfeits reach consumers.

The SHOP SAFE Act of 2020 represents Congress’ most bipartisan and comprehensive proposal to address the problem of counterfeit goods sold by third-party sellers on e-commerce platforms. The bill is commendable for proposing a viable solution to the twin problems faced by consumers and brand owners seeking to stop third-party sellers from peddling illicit goods online: (1) how to identify third-party sellers using e-commerce platforms for illegal purposes and (2) how to prevent third-party sellers from using e-commerce platforms to facilitate the sale of

126 Id. at Sec. 4(A)(ii)(VII)-(VIII).
127 Id. at Sec. 4(A)(ii)(II), (III)(aa).
128 Id. at Sec. 4(A)(ii)(V).
129 Id. at Sec. 4(A)(ii).
counterfeit goods *before* such sellers list or sell counterfeits on these platforms. In proposing the SHOP SAFE Act of 2020, Congress understands that e-commerce platforms are in the best position to solve both these problems. It also demonstrates that Congress – like the Oberdorf panel, brand owners, consumers, DHS, and the President did before the bill was proposed – also recognizes that the e-commerce platforms’ current business models emphasizing after-the-fact, whack-a-mole approaches neither protect consumers nor deter third-party sellers from using the platforms to sell counterfeit goods. For these reasons, passage of the SHOP SAFE Act of 2020 would represent a significant step toward stemming the rising tide of counterfeit goods sold by third-parties on e-commerce platforms.

Nevertheless, the bill could be strengthened by amending it to address at least two areas. *First*, the bill limits its imposition of contributory liability to “goods that implicate health and safety.” The bill defines this phrase as including goods that “can lead to illness, disease, injury, serious adverse event, allergic reaction, or death if produced without compliance with all applicable [government] regulations and industry-designated testing, safety, quality, certification, manufacturing, packaging and labeling standards.”

Although it will be relatively easy for e-commerce platforms to identify certain types of goods as those “that implicate health and safety” – like medicine or perfumes – other goods will be more difficult. For example, at first glance, a simple office chair does not seem like it would implicate health and safety. However, a counterfeit office chair that breaks could cause someone to injure themselves. What about the retractable dog leash in Oberdorf? Before that case, many might argue that a retractable dog leash would not meet the bill’s definition of a good implicating health and safety.

Ultimately, it would be easier for e-commerce platforms to implement the bill’s due diligence requirements if they apply to all goods sold by third-party sellers on the platforms. Asking e-commerce platforms to distinguish between goods that do implicate health and safety from those that do not will be a difficult and time-consuming task at best. In the typical third-party seller context, e-commerce platforms will never see the physical product being sold because the third-party seller directly sells the good to the consumer. In addition, determining which goods meet the definition will likely lead to unnecessary litigation that could water-down the effectiveness of the bill. Applying the bill to all goods sold by

---

130 *Id.* at Sec. 4(B)(iii).
third-parties solves these problems. After all, consumers are entitled to buy the authentic goods they are seeking. They should be confident that every category of goods they buy on e-commerce platforms will be authentic.

Second, the bill’s requirement that e-commerce platforms verify the identity of third-party sellers could be strengthened. Relying on government identifications may be reasonable when that identification comes from a reliable governmental entity (like a state’s Department of Motor Vehicles) in the U.S. that can be verified. However, many third-party sellers are not U.S.-based, and not every country’s identification will be able to be checked against that country’s government database or have similar reliability. For third-party sellers based overseas, more reliable forms of identification may include a third-party seller’s:

(1) business license to prove it is lawfully registered to do business;
(2) bank account certificate to show the seller’s real overseas bank account; and
(3) foreign trade registration certificate to ensure the company is registered for overseas trade.

Including these types of government identification in the bill as part of a non-exclusive list of forms of identification will make clear that reliable identification will not always be an overseas driver’s license or country identification.

C. INFORM Consumers Act

The Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers (“INFORM Consumers”) Act was introduced into the Senate on March 10, 2020. The bill’s intent is to require e-commerce markets to vet high volume third-party sellers. E-commerce platforms will be required to publish on an annual basis the full name of the seller, the full business address of the seller, whether the seller engages in the manufacturing, importing, retail, or reselling of consumer products, and the contact information for the seller. INFORM

131 INFORM Consumers Act, S.3431 — 116th Congress (2019-2020), March 10, 2020 (Cassidy R-LA), sponsored by Senator Bill Cassidy [R-LA], and co-sponsored by Senators Richard Durbin [D-IL], David Perdue [R-GA], and Mazie Hirono [D-HI].

132 Id.

133 Id. at Sec. 2.
Consumers Act shares many of the provisions of the SANTA Act and was introduced by the same Senator. For example, like the SANTA Act, violations of the INFORM Consumers Act would constitute an unfair and deceptive practice under the Federal Trade Commission Act.134

However, the INFORM Consumers Act goes beyond the SANTA Act by covering all consumer products – not just toys.135 The INFORM Consumers Act also aimed to address some of the concerns raised by the January 2020 DHS Response to the President’s Memorandum136 – which came out after the SANTA Act.

While the INFORM Consumers Act covers all consumer products, the bill limits its application to high volume third-party sellers.137 The Act defines a “high-volume third party seller” as a third-party seller “who, in any continuous 12-month period during the previous 24 months, has entered into 200 or more discrete sales or transactions of new or unused consumer products resulting in the accumulation of an aggregate total of $5,000 or more in gross revenues.”138 The bill does not go into detail about who is responsible (the seller or the platform) for determining who is a high-volume third party seller, what happens when an IP rights owner discovers a high-volume seller who is not currently on this list, or whether the scale requirements necessary to be a high volume seller are calculated based on one platform, or various versions of a platform that may have different applications (such as the Alibaba suite of platforms).

Additionally, the Act allows for exceptions. For instance, if the high-volume third-party seller only lists a personal address, then the seller can have the exact address withheld and only disclose the country or state in which they reside –

134 INFORM Consumers Act, at Sec. 2(d) (noting “A violation of subsection (a), (b), or (c) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))).”
135 Id. at Sec 2(e)(2).
137 Id.
138 Id. at Sec. 2(e)(3).
limiting consumers to sending their inquiries to the email address on record.139 Likewise, if the seller does not have a work phone number, then consumers would be directed, again, to the seller’s email address.”140 While these exceptions seem practical, they err on the side of the third-party high-volume seller and not the consumer. Many of the problems that already exist currently have to do with sellers with email addresses that cannot be located when their products are found to be fraudulent or counterfeit, or when the sellers do not have legitimate businesses. These exceptions tend to perpetuate this problem.

One important limitation to this exception does exist: when an online marketplace becomes aware of a false representation by the third-party seller, or has failed to disclose the required answers within a reasonable time for partial disclosure, then the seller must provide full disclosure of the seller’s contact information within three days of notice.141 This provision also does not specify who the onus is on to discover false representations—should the platforms be actively trying to confirm that the representations are true, or are they exempt from any liability by any disclosure from a third-party seller.

This leads to one of the fundamental problems with the reporting requirement for the INFORM Consumers Act and the SANTA Act – reliance on the use of verification documents. There is no detail in these acts about whether the simple submission of the listed verification documents is enough to waive liability of the platforms for unfair or deceptive practices, or if there is an assumed responsibility for the platforms to somehow verify that the documents are authentic and are actually being used by those selling the goods.

III. How Congress Can More Effectively Stop Counterfeiting in E-Commerce

What Congress has proposed so far to combat counterfeiting in e-commerce is commendable. Congress deserves recognition for its bipartisan effort to protect consumers from third-party sellers who are intent on selling counterfeits for a quick profit, and to encourage e-commerce platforms to adopt business models that

139 Id. at Sec. 2(b)(2)(i).
140 Id. at Sec. 2(b)(2)(ii).
141 Id. at Sec. 2(b)(2)(B).
take proactive steps to prevent counterfeits from ever being listed or sold on their platforms. Nonetheless, we recommend some simple steps Congress can take to improve its efforts.

A. Harmonize the type of goods

First, Congress should harmonize these bills into one bill to make it easier for e-commerce platforms to comply with them. For instance, each of the bills requires e-commerce platforms to distinguish certain types goods or third-party sellers from others – whether its toys vs. non-toys (the SANTA Act), goods the implicate health and safety vs. goods that do not (the SHOP SAFE Act of 2020), or high-volume third-party sellers vs. low-volume third-party sellers (the INFORM Consumers Act). Asking e-commerce platforms to make these distinctions invites litigation over how they make these decisions instead of taking the shortest path to each bill’s goal of keeping counterfeit goods off e-commerce platforms. Sometimes the best solution is the simplest: enact one bill that requires e-commerce platforms to apply the same verification and due diligence requirements for all types of goods sold be all third-party sellers.

B. Technology Neutral

Second, Congress should enact one comprehensive bill that is technology neutral. The dramatic growth of e-commerce and its nefarious uses has come upon the U.S. legal system quickly. With new legislation in the era of technology, thought and consideration needs to be given to whether it will be a valid useful legal framework five years from now, ten years from now, or twenty years from now. E-commerce and the surrounding technologies that are being used with it, such as artificial intelligence, are “law disruptive technologies”. Nevertheless, requiring e-commerce platforms to use “proactive technological measures” and other “technological measures” dependent on artificial intelligence makes little sense if the e-commerce platforms have a non-technological proactive measure that may be more effective in preventing the sale of counterfeits on their platforms. In

the same vein, specifying use of a particular technology would be problematic if in five to ten years from now another more effective technology comes to market.

C. Clear Verification and Identification Requirements

Third, Congress should enact one bill that includes clear, but rigorous, requirements for e-commerce platforms to verify and to disclose the identity of a third-party seller, regardless of whether they are a business or an individual, before the seller may list any products on the platform. In fact, and perhaps in reaction to the identification requirements already proposed in these three bills, e-commerce platforms have already started to publicly share the identity of third-party sellers. For instance, on July 8, 2020, Amazon announced that, starting on September 1, 2020, it will require third-party sellers in its U.S. marketplace to display their business name and address on their public-facing profiles.  

Although it is not reasonable for Congress to list every form of reliable identification, it can require e-commerce platforms to obtain enough information about a third-party seller to allow a consumer, brand owner, or law enforcement to serve federal process on a third-party seller who sells illicit goods. This is the bare minimum that should be required. However, this requirement for the base level of information for serving federal process is also the simplest for e-commerce platforms to implement and distills the most important identification information for consumers and brand owners. Most important, this approach refocuses the verification requirement on the real goal of these bills – to provide e-commerce platforms with a safe harbor from secondary liability in exchange for providing consumers, brand owners, and law enforcement with the information needed to go after third-party sellers who would sell illicit or counterfeit goods. If the information obtained by the e-commerce platform is insufficient to allow injured parties or law enforcement to find and serve third-parties who sell counterfeit or other illicit goods, then the platform should lose its safe harbor and be subject to liability. The SHOP SAFE Act of 2020 comes closest to implementing this recommendation.

D. Due Diligence Requirements of E-Commerce Platforms

Fourth, Congress should enact one bill that imposes a comprehensive list of due diligence requirements on e-commerce platforms to detect counterfeit and illicit goods proactively, or before a third-party seller can list its goods on the platform. For example, Congress should require e-commerce platforms to determine whether a third-party seller has a history of selling illicit goods. This first step is helpful, but it does not prevent the individuals behind a company from playing a shell game by constantly creating new entities. Thus, Congress should also require e-commerce platforms to determine whether the individuals behind a third-party seller—whether as individuals or as operators of other entities—have their own history of selling illicit goods before allowing them to sell goods on their platforms.

E. Type of Liability Imposed

Fifth, Congress should enact one bill that focuses on imposing secondary liability on e-commerce platforms based on counterfeit trademark and strict liability theories. Imposing liability based on the unfair trade or deceptive practices act is insufficient to cover the types of harms caused by third-parties who sell illicit goods.

IV. Conclusion

In proposing the SANTA Act, the SHOP SAFE Act of 2020, and the INFORM Consumers Act, Congress has taken an important first step to protecting consumers from third-party sellers who would use e-commerce platforms to sell counterfeit and other illicit goods. As e-commerce continues to explode in growth, Congress must take the next step of enacting a comprehensive, technology neutral Act that motivates e-commerce platforms to take the proactive steps necessary to identify third-party sellers and to detect counterfeit goods before third-party sellers have the chance to use their platforms for illicit purposes.