IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

EDWARD WARGO, Plaintiff, v. SCHEDULE A DEFENDANTS, Defendants.	Civil Action No. 26-cv-190 **FILED UNDER SEAL**

DECLARATION OF STANLEY D. FERENCE III IN SUPPORT OF PLAINTIFF'S *EX PARTE* APPLICATION FOR ENTRY OF A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

I, STANLEY D. FERENCE III, hereby declare as follows:

1. I am an attorney with the law firm of Ference & Associates LLC ("the Ference Firm"), located at 409 Broad Street, Pittsburgh, Pennsylvania 15143 and represent Plaintiff in the above-referenced action.

2. I make and submit this declaration in support of Plaintiff's *ex parte* application for the following: 1) a temporary restraining order; 2) an order restraining assets and Merchant Storefronts; 3) an order to show cause why a preliminary injunction should not issue; and 4) an order authorizing expedited discovery against the above-named Defendants, Third Party Service Providers, and Financial Institutions, in light of Defendants' intentional and willful offerings for sale and/or sales of Infringing Products ("Application").

Document Authentication

3. According to the Fiscal Year 2021 U.S. Customs and Border Protection ("CBP") Intellectual Property Seizure Statistics Report, e-commerce sales have resulted in a sharp

increase in the shipment of unauthorized products into the United States. Over 89% of all CBP intellectual property seizures were smaller international mail and express shipments (as opposed to large shipping containers). *Id.* Over half (51%) of CBP seizures originated from mainland China and Hong Kong. *Id*. A true and correct copy of an excerpt of this report is attached hereto as **Exhibit 1**.

4. According to Daniel C.K. Chow, in "Alibaba, Amazon, and Counterfeiting in the Age of the Internet," 40 NW. J. INT'L L. & BUS. 157, 186 (2020), third-party service providers do not adequately subject new sellers to verification and confirmation of their identities, allowing counterfeiters to "routinely use false or inaccurate names and addresses when registering with these e-commerce platforms." Further, "E-commerce platforms create bureaucratic or technical hurdles in helping brand owners to locate or identify sources of counterfeits and counterfeiters*"* (pages 186-187). A true and correct copy of this report is attached hereto as **Exhibit 2**.

5. A report on "Combating Trafficking in Counterfeit and Pirated Goods" prepared by the U.S. Department of Homeland Security's Office of Strategy, Policy, and Plans (Jan. 24, 2020) finds that on "at least some e-commerce platforms, little identifying information is necessary for a counterfeiter to begin selling" and recommending that "[s]ignificantly enhanced vetting of third-party sellers" is necessary. Counterfeiters hedge against the risk of being caught and having their websites taken down from an e-commerce platform by preemptively establishing multiple virtual store-fronts. Since platforms generally do not require a seller on a third-party marketplace to identify the underlying business entity, counterfeiters can have many different profiles that can appear unrelated even though they are commonly owned and operated. A true and correct copy of this report is attached hereto as **Exhibit 3**.

Rule 65(b) Certifications

6. In my experience policing the Plaintiff's products and based upon my review of lawsuits filed by other brand owners, sellers of counterfeit and/or infringing products, particularly those sellers whose product listings are removed, merely change the description or photograph and then re-post the listing for the products on their respective Merchant Storefront[1] or modify or create a new User Account[2] and/or Merchant Storefront and proceed to sell the same product again. Likewise, these counterfeit sellers are sophisticated enough to monitor the US courts through PACER and the like looking for lawsuits that name them or their associates Merchant Storefronts and will drain their related financial accounts upon any notice that a lawsuit is filed against their activity.

7. Based upon my personal experience and my review of lawsuits filed by other brand owners, I have learned that the Defendants selling on online marketplaces do not display their registered business name or trade name, contact name, complete address, phone numbers, or any other contact information. These Defendants use their respective Merchant Storefronts and User Accounts to anonymously sell their Infringing Products.[3] Likewise, these Defendants typically use shipping services like EMS and DHL and ePacket. These shipping services provide

---

1 As defined in the Complaint, a "User Account" is any and all accounts with online marketplace platforms such as, Amazon.com and Walmart.com, as well as any and all as yet undiscovered accounts with additional online marketplace platforms held by or associated with Defendants, their respective officers, employees, agents, servants and all other persons in active concert with any of them.

2 As defined in the Complaint, a "Merchant Storefront" is any and all User Accounts through which Defendants, their respective officers, employees, agents, servants and all persons in active concert or participation with any of them operate storefronts to manufacture, import, export, advertise, market, promote, distribute, display, offer for sale, sell and/or otherwise deal in products, including Infringing Products, which are held by or associated with Defendants, their respective officers, employees, agents, servants and all persons in active concert or participation with any of them.

3 As alleged in the Complaint, Defendants are using without authorization Plaintiff's Works. Defendants are manufacturing, importing, exporting, advertising, marketing, promoting, distributing, offering for sale and/or selling unlicensed products that infringe Plaintiff's Works.

minimal tracking and/or use incomplete or made-up return addresses to further secret their identities.

Based upon the foregoing facts and supported by the evidence, including the Declarations of Edward Wargo, and Dee Odell, it is submitted that providing notice of the Motion for Temporary Restraining Order and the restraints of the Defendants' Merchant Storefronts and Accounts would allow the Defendants to avoid the Court's Order thus depriving the Plaintiff of any damage recovery and otherwise prevent the full operation of the Court's Order.

8. To prevent the Defendants from escaping the effects of the Court's Order, Plaintiff, Plaintiff's Counsel and their agents have not publicized the filing of this lawsuit or the request for *ex parte* relief.

9. It is respectfully submitted that based upon the Complaint allegations, and the declarations and exhibits submitted therewith, Plaintiff has met the requirements of Fed. R. Civ. P. 65 (b) in its application to the court for an Ex Parte Temporary Restraining Order because:

(a) the specific facts in the affidavit and the complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and

(b) the movant's attorney (undersigned) has herein certified in writing that notice would, in this case, defeat the purposes of the application for the *ex parte* temporary restraining order and asset restraint.

Jurisdiction Over Online Marketplaces and Financial Institutions

10. Defendants at least use the Third Party Service Providers Amazon.com, Temu, and Walmart.com to support and drive consumer traffic to their counterfeiting operation.

Defendants also use the services of the Financial Institutions Amazon pay, PayPal, and Walmart Pay operated by Wal-Mart.com USA, LLC (as more fully described below) to transmit money derived from their transactions on the Third Party Platforms. Based upon my own research, experience, and communications with various Parties to be enjoined, the paragraphs below set forth my information and belief about the identity of each, service addresses, and willingness to accept service, submit to jurisdiction of this court, and comply with court any orders.

11. Based upon my own research and a review of pleadings (including declarations) in multiple past actions by other brand owners, as described above, Amazon.com is an online marketplace and e-commerce platform that is owned and operated by Amazon.com, Inc. and its affiliate, Amazon Services LLC, a Nevada Corporation, with a registered address of Corporation Service Company, is a foreign registered corporation in the Commonwealth of Pennsylvania with a registered address of c/o Corporation Services Company, Dauphin County and 300 Deschutes Way, SW, Suite 304, Tumwater, WA 98501, ATTN: Legal Department. As such, the Court has jurisdiction over Amazon Services LLC.

12. Wal-Mart.com USA, LLC is a foreign registered corporation in the Commonwealth of Pennsylvania with a registered address of "c/o CT Corporation System Allegheny, 600 North 2nd Street, Suite 401, Harrisburg, Pennsylvania 17101." Wal-Mart's legal team has indicated by email that it will cooperate with any court order issued by this Court.

13. Amazon is an e-commerce marketplace that allows Defendants to conduct their commercial transactions privately via Amazon's payment processing and retention service, Amazon Payments, Inc. As such, Defendants' payment information is not publicly disclosed. I know from multiple past actions filed by brand owners that counterfeiters do not identify the payment accounts they are using in attempts to evade detection. Because Amazon also operates

as a money transmitter for sales made on Amazon, however, it has the ability to identify and restrain the payment accounts associated with Defendants. Amazon Payments, Inc. admits on its website, https://pay.amazon.com/us/help/82972 (last accessed on January 7, 2026), it is a licensed money transmitter under Pennsylvania's Transmitting Money Act (License #17489). As such, this Court has jurisdiction over Amazon Payments, Inc.

14. PayPal, Inc. is foreign registered corporation in the Commonwealth of Pennsylvania with a registered address of "c/o CT Corporation System Dauphin" which indicates "c/o C T Corporation System, 600 North 2nd Street, Suite 401, Harrisburg, Pennsylvania 17101." According to PayPal's website at https://www.paypal.com/us/webapps/mpp/licenses (last accessed on January 7, 2026), it is a licensed money transmitter under Pennsylvania's Transmitting Money Act (License #0043). As such, this Court has jurisdiction over PayPal, Inc.

15. Wal-Mart.com operated by Walmart Inc. and Wal-Mart.com USA, LLC (collectively "Walmart") is an e-commerce marketplace that allows Defendants to conduct their commercial transactions privately via Walmart's payment processing and retention service, Walmart Pay. As such, Defendants' payment information is not publicly disclosed. I know from multiple past actions filed by brand owners that counterfeiters do not identify the payment accounts they are using in attempts to evade detection. Wal-Mart.com, however, has the ability to identify and restrain the payment accounts associated with Defendants and has indicated that it will cooperate with counsel to comply with any restraining orders.

16. Klarna, Inc. is foreign registered corporation in the Commonwealth of Pennsylvania with a registered address of "c/o CT Corporation System Dauphin" which indicates "c/o C T Corporation System, 600 North 2nd Street, Suite 401, Harrisburg, Pennsylvania 17101." According to NMLS's website at

https://www.nmlsconsumeraccess.org/EntityDetails.aspx/COMPANY/1353190 (last accessed on January 7, 2026), it is a licensed money transmitter under Pennsylvania's Transmitting Money Act (License #60039). As such, this Court has jurisdiction over Klarna, Inc.

17. Temu Marketplace is owned and operated by Whaleco Inc., a Delaware Corporation, which is a wholly owned subsidiary of Pinduoduo Inc. which is owned by PDD Holdings (collectively, "Temu"). Temu has the ability to identify owners of Temu storefronts, restrain seller's accounts and take down infringing listings. Temu has confirmed for Plaintiff's counsel that it will comply with any court orders issued against sellers on the Temu Marketplace.

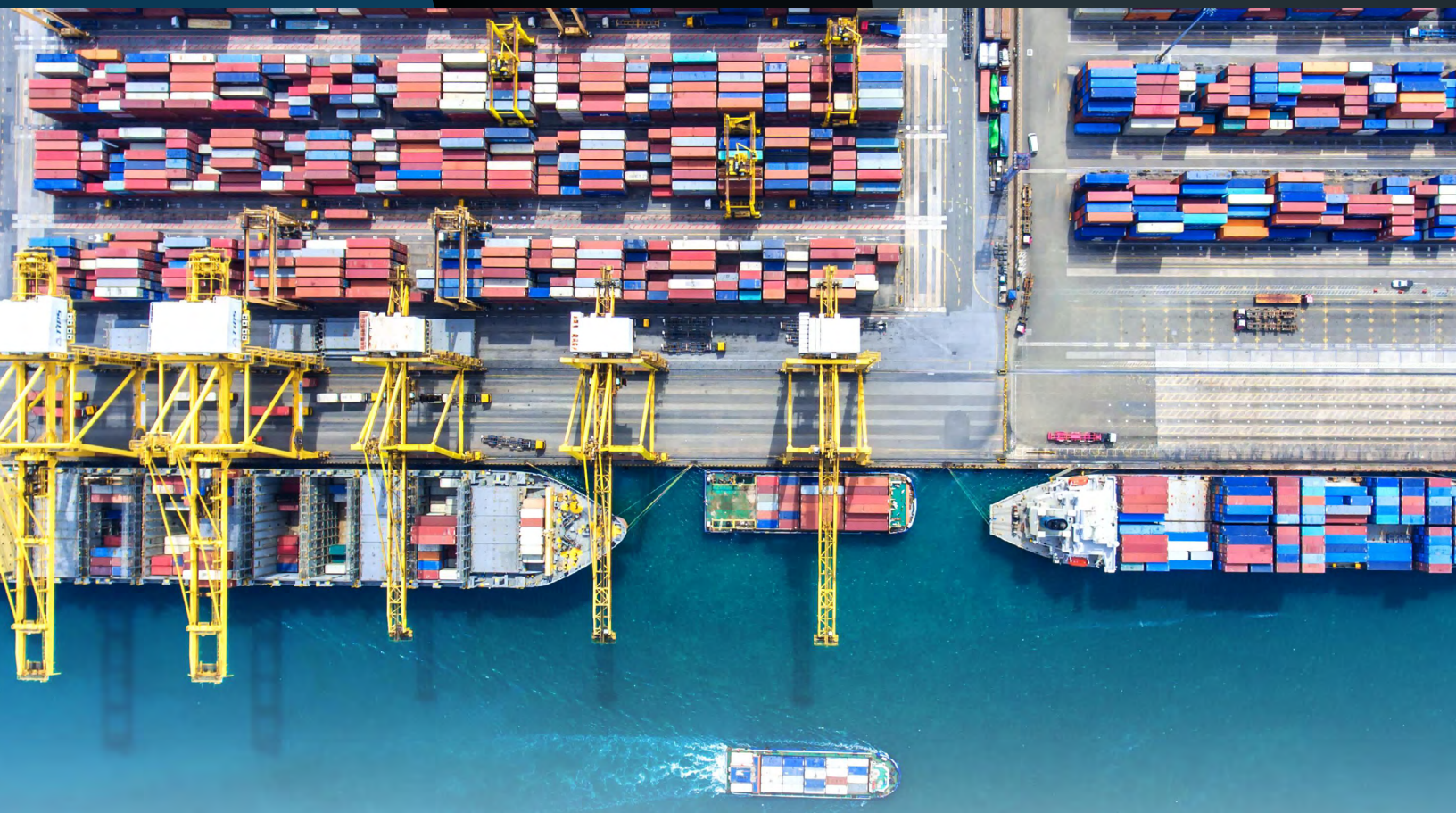
I declare under penalty of perjury that the foregoing is true and correct.

Dated: Pittsburgh, Pennsylvania
February 3, 2026

/Stanley D. Ference III/
Stanley D. Ference III

EXHIBIT 1

Intellectual Property Rights Seizure Statistics



U.S. Customs and Border Protection

Fiscal Year 2021

Contents

Executive Summary 5

IPR Seizure Totals 5

Counterfeit Commodity Spotlight – Cell Phones and Accessories 6-7

COVID-19 Spotlight 9

Operational and Enforcement Highlights 11

CBP Partnerships 12-15

Help CBP Protect American Ingenuity 17

Exclusion Orders and Outreach 19

Outreach: CBP/U.S. Chamber of Commerce Memorandum of Understanding 20

Outreach: The Year of the Small and Medium Sized Enterprises Webinar Series 21

IPR and E-Commerce 23-24

Centers of Excellence and Expertise Spotlight 25

Mode of Transportation and Top Product Commodities 27

Seizure World Map 28-29

Number of Seizures 30-31

Products Seized by MSRP 32-33

Total Seizure Lines and MSRP Seized by Economy 34-35

Seizures by Mode of Transportation 36-37

Health, Safety, and Security by Product 38-39

MSRP by Centers of Excellence and Expertise 40-41

CBP IPR Points of Contact 42-43

Disclaimer: The information contained in this report does not constitute the official trade statistics of the United States. The statistics, and the projections based upon those statistics, are not intended to be used for economic analysis, and are provided for the purpose of establishing U.S. Department of Homeland Security workload.

Mode of Transportation and Top Product Commodities

SEIZURES BY MODE OF TRANSPORTATION

16,926 EXPRESS

7,293 MAIL

2,274 CARGO

ALL OTHERS 622

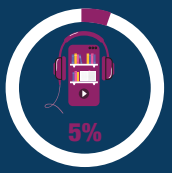
TOP PRODUCTS SEIZED BY NUMBER OF SEIZURE LINES

30% WEARING APPAREL/ ACCESSORIES

28% HANDBAGS/ WALLETS

13% FOOTWEAR

12% WATCHES/ JEWELRY



5% CONSUMER ELECTRONICS

4% CONSUMER PRODUCTS

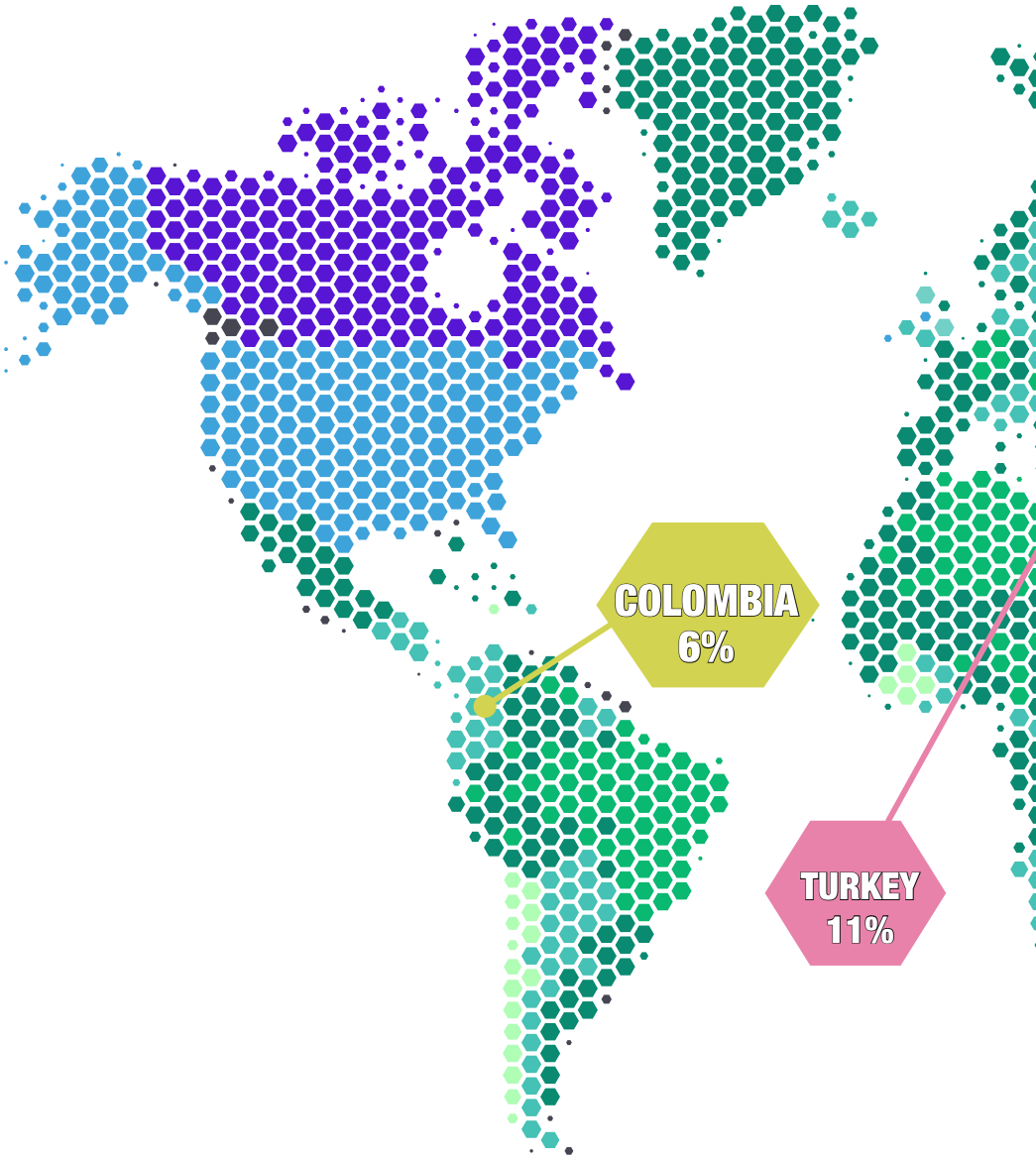
3% PHARMACEUTICAL/ PERSONAL CARE

1% AUTOMOBILE/ AEROSPACE

1% LABEL TAGS

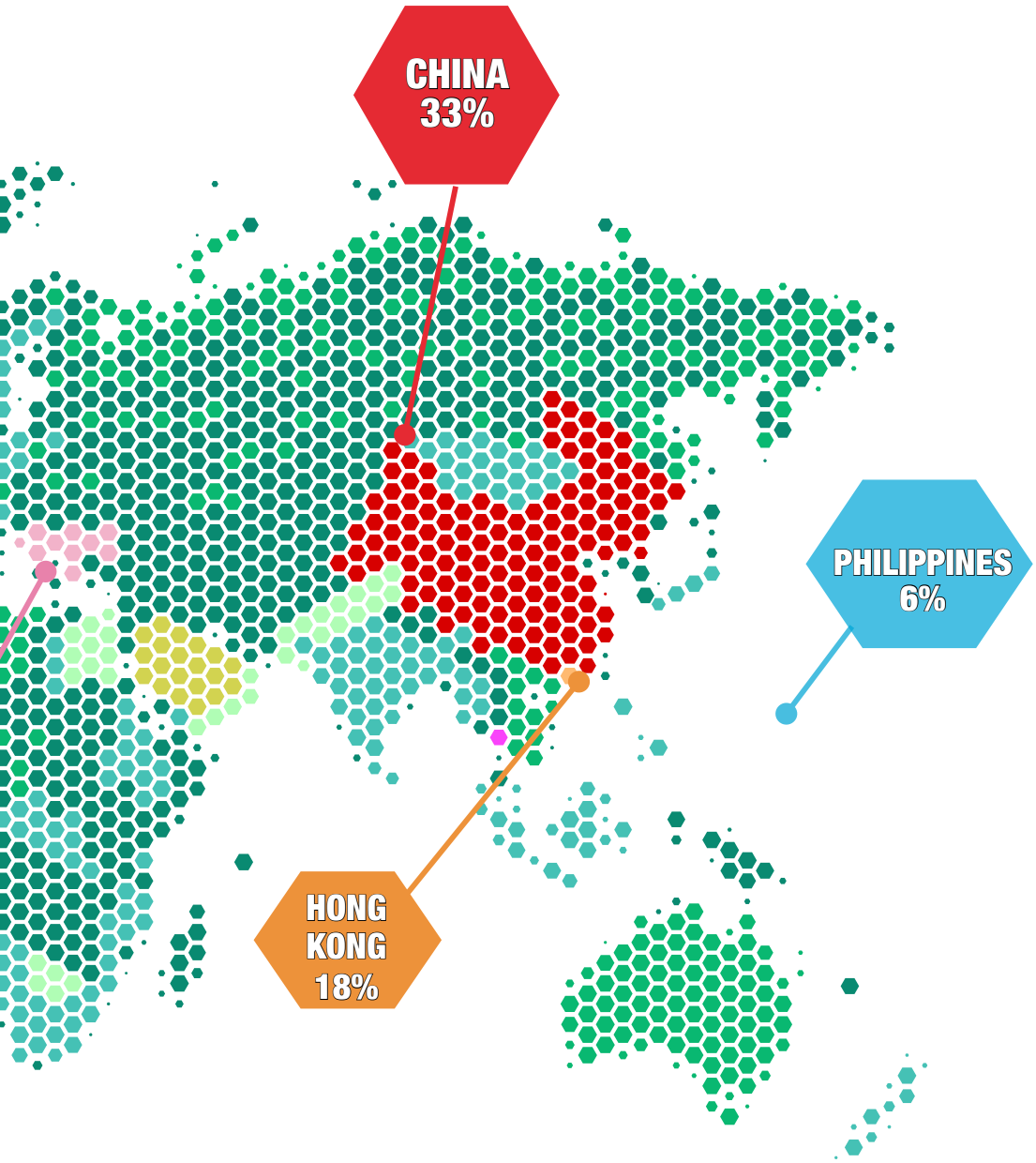
ALL OTHER COMMODITIES 4%

Seizure World Map



FY 2021 TOTALS
NUMBER OF SEIZURE LINES: 102,490
MSRP: $3.3 Billion

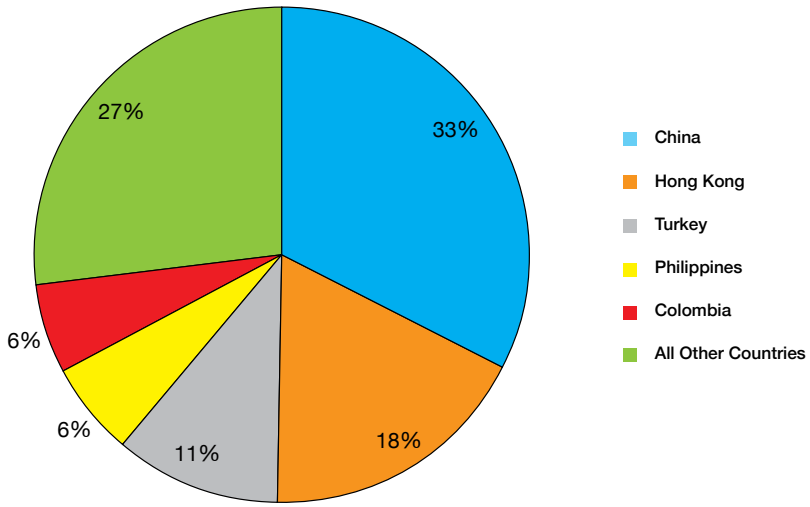
Seizure World Map



ALL OTHER COUNTRIES 27%

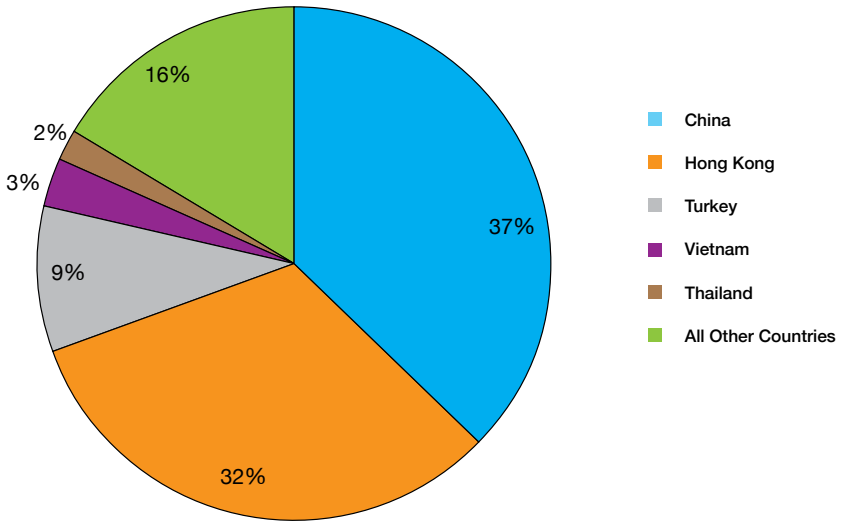
Total Seizure Lines and MSRP Seized by Economy

Seizure Lines By Economy FY 2021



Number of Seizure Lines: 102,490

Seizure Lines By Economy FY 2020



Number of Seizure Lines: 72,357

Total Seizure Lines and MSRP Seized by Economy

Seizures Lines and Related MSRP by Economy – FY 2021			
Trading Partner	**Seizure Lines**	**% of Total**	**MSRP**
China	33,323	33%	$1,888,298,761
Hong Kong	18,466	18%	$613,462,655
Turkey	10,781	11%	$60,347,048
Philippines	6,416	6%	$45,692,010
Colombia	5,912	6%	$23,980,798
All Other Countries	27,592	27%	$698,256,079
Total	**102,490**	**100%**	**$3,330,037,350**

Seizures Lines and Related MSRP by Economy – FY 2020			
Trading Partner	**Seizure Lines**	**% of Total**	**MSRP**
China	26,985	37%	$660,767,476
Hong Kong	23,493	32%	$428,961,694
Turkey	6,831	9%	$31,237,035
Vietnam	2,123	3%	$25,803,755
Thailand	1,445	2%	$12,601,807
All Other Countries	11,480	16%	$149,784,743
Grand Total	**72,357**	**100%**	**$1,309,156,510**

* The aggregate seizure data reflect the reported country of origin, not necessarily where the seized goods were produced. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100 percent.

EXHIBIT 2

Northwestern Journal of International Law & Business

Volume 40
Issue 2 *Winter*

Article 1

Winter 2020

Alibaba, Amazon, and Counterfeiting in the Age of the Internet

Daniel C.K. Chow

Follow this and additional works at: https://scholarlycommons.law.northwestern.edu/njilb

Part of the International Trade Law Commons, and the Internet Law Commons

Recommended Citation

Daniel C.K. Chow, *Alibaba, Amazon, and Counterfeiting in the Age of the Internet*, 40 NW. J. INT'L L. & BUS. 157 (2020).
https://scholarlycommons.law.northwestern.edu/njilb/vol40/iss2/1

This Article is brought to you for free and open access by Northwestern Pritzker School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of International Law & Business by an authorized editor of Northwestern Pritzker School of Law Scholarly Commons.

Copyright 2020 by Daniel C.K. Chow
Vol. 40, No. 2
Northwestern Journal of International Law & Business

ALIBABA, AMAZON, AND COUNTERFEITING IN THE AGE OF THE INTERNET

Daniel C.K. Chow*

Abstract:

The advent of e-commerce marketplaces such as Alibaba and Amazon in the new millennium has led to the proliferation of the sale of counterfeit goods around the world through the Internet. Brand owners find that Internet counterfeiters operating in the digital world present even more challenges than those using only brick-and-mortar operations. Internet counterfeiters have unprecedented access to consumers. They use false identities and addresses and vanish into cyberspace at the first sign of trouble. Brand owners seeking help from Alibaba and Amazon to remove listings of counterfeits have become frustrated by their convoluted and labyrinthine notice and take-down procedures. Even when these procedures are used successfully, brand owners find that the process can take months only to have the counterfeiter reappear in short order using a new false identity. Many brand owners find that dealing with Alibaba and Amazon only adds to their misery and believe that both tolerate counterfeits as they earn revenue from all sales, including sales of counterfeit goods.

This Article sets forth for the first time how brand owners can use a set of currently available information technology tools to help create an effective deterrent to counterfeits on the Internet. Using these tools, brand owners can force counterfeiters to abandon the subterfuge and disguise that they rely on so that brand owners can—without the assistance of e-commerce platforms—directly pursue counterfeiters in civil and criminal actions in China where most of the counterfeiters are located and in the United States. The proposed approach should help deter counterfeiters who always work in secrecy and disguise by

* B.A., JD, Yale University. Bazler Chair in Business Law, The Ohio State University Michael E. Moritz College of Law. The author lived and worked in China as head of the legal department for a multinational company in the consumer products business with serious counterfeiting issues. The author also helped to organize and served as the first executive secretary for the China Anti-Counterfeiting Coalition, a lobby group for multinationals in China (now known as the Quality Brands Protection Committee), and was the principal author of the white paper on counterfeiting in China commissioned by the PRC State Council. More recently, in addition to academic duties, the author served as an attorney and expert witness in U.S. litigation involving the sale of counterfeit cigarettes and internet e-commerce sites in China and the United States. The opinions expressed in this Article are the author's own but the author has profited from many discussions with colleagues. The author also thanks Natasha Landon, Moritz Law Librarian for her excellent research help.

exposing them to what they fear and loathe the most: transparency and accountability for their illegal actions.

TABLE OF CONTENTS

I. Introduction 160
II. Counterfeiting and the Internet 167
A. Brief Overview of Counterfeiting in China 167
B. The Advent of the Internet 168
C. Liability Regimes for Internet Service Providers 171
D. Alibaba 172
1. Brand Owner Concerns 172
a. Alibaba's Defense of Counterfeits 175
b. Counterfeits for Sale on Alibaba 176
2. Alibaba's "Arrogance" and Illegal Activities 179
a. Specific Practices 181
b. Above the Law in China 183
E. Amazon 184
III. Entity Verification Measures and the Requirements of PRC Law 186
A. Problems with Enforcement 186
1. False Names, Identities, and Addresses. 186
2. Burdensome Notice and Takedown Procedures 186
3. Lack of Deterrence 187
B. Proposed Remedial Measures 188
1. AIC Business License 188
2. Legal Representative 190
3. Verification and Deterrence 192
4. Amazon and PRC Law 193
5. Consent to Arbitration before CIETAC 194
IV. Conclusion 195
V. Appendices 199
Appendix 1. Alibaba Listing: Gucci Guccio Handbags 199
Appendix 2. Alibaba Listing: Hennessy XO 200
Appendix 3. Alibaba Listing: Abercrombie & Fitch Sweatpants 201
Appendix 4. Abercrombie & Fitch Sweatpants 202

I. INTRODUCTION

The advent of internet commerce (e-commerce) in the early 2000s coincided with the unprecedented and historic rise of counterfeiting in the People's Republic of China (PRC or China) that had begun in the 1990s.[1] Although sales of counterfeits through brick-and-mortar establishments had already gained a substantial share of the market in China by the early 2000s,[2] the rise of the Internet in the new millennium has allowed counterfeiters in China unparalleled access to consumers not just in China but also in the United States and worldwide by transcending the physical limitations inherent in the use of brick-and-mortar operations.[3] Recent studies show that counterfeits and infringing products have proliferated on the Internet and have reached levels of saturation that were unattainable by counterfeiters selling through brick-and-mortar distributors.[4] For example, Xinhua, China's official news agency stated that more than 40% of all goods sold online through Chinese e-commerce platforms in a recent year were "counterfeits or of bad quality."[5] Since Xinhua is controlled by the Communist Party of China (the Party) and would want to present China in the best light possible, the 40% figure might understate the severity of the problem. Most consumers in China believe that the likelihood of a product sold on the Internet is counterfeit is very high, and those who wish to buy genuine products avoid the use of the Internet altogether.[6] This 40% figure cited by Xinhua is double the estimated 15-20% rate of counterfeits sold in brick-and-mortar establishments in China.[7] In the United States, the U.S. General Accounting Office recently conducted a study and found that among a selection of 47 items belonging to four types of frequently counterfeited goods (i.e., sneakers, mugs, cosmetics, and phone chargers) purchased online, 27 were

---

[1] *See* Daniel C.K. Chow, *Counterfeiting in the People's Republic of China*, 78 WASH. U.L Q. 1, 3 (2000).

[2] By the early 2000s, brand owners estimated that counterfeits comprised 15-20% of all goods sold on the market in China. *See id.* at 3 n.3 (citing Joseph T. Simone, *Countering Counterfeiters*, CHINA BUS. REV., Jan. 1, 1999, at 12).

[3] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-216, INTELLECTUAL PROPERTY: AGENCIES CAN IMPROVE EFFORTS TO ADDRESS RISKS POSED BY CHANGING COUNTERFEITS MARKET 11 (2018), https://www.gao.gov/assets/690/689713.pdf (discussing how the use of the internet allows counterfeiters to transcend limits of brick and mortar counterfeiting) [hereinafter GAO REPORT].

[4] *See infra* Parts II.A & II.B.

[5] *More than 40 Per Cent of China's Online Sales 'Counterfeits or Bad Quality'*, TELEGRAPH (Nov. 3, 2015), https://www.telegraph.co.uk/news/worldnews/asia/china/11971401/More-than-40-per-cent-of-Chinas-online-sales-counterfeit-or-bad-quality.html. Xinhua does not distinguish between counterfeits and products of poor quality; it is unclear whether Xinhua believes that these are two separate categories of goods or a single category as most counterfeits are of poor quality.

[6] This observation is based upon the author's own experience living and working in China and on discussions with colleagues and associates.

[7] *See* Chow, *supra* note 1, at 3 n.3.

authentic and 20 were counterfeit.[8] After Seattle-based Amazon made efforts in 2015 to woo Chinese manufacturers to sell directly on its platform, complaints about counterfeits and infringing products sold on Amazon have risen sharply.[9]

Efforts by multinational companies (MNCs) that own trademarks (or brands), copyrights, and other intellectual property rights to stem the flow of counterfeits through the Internet have been largely unsuccessful, leading to anger and frustration.[10] Under current legal regimes, e-commerce platforms are in general not liable for counterfeits sold by third-party online vendors using the site;[11] liability lies with the vendor itself, but many brand owners argue that Internet commerce sites facilitate the sales of counterfeits.[12] E-commerce platforms earn revenues from sales, including sales of counterfeits.[13] Many brand owners argue that e-commerce platforms facilitate counterfeiting by allowing webpages or postings of counterfeit goods to remain on their sites despite the many protests of brand owners.[14] Some of these offending webpages are removed after brand owners suffer through a long and convoluted notice and takedown procedure only to reappear under a new false name and address in short order.[15] In China,

---

[8] *See* GAO REPORT, *supra* note 3, at 15. The products were Nike Air Jordan shoes, Yeti travel mugs, Urban Decay cosmetics, and UL-certified phone chargers. *Id.*

[9] Wade Shepard, *How Amazon's Wooing of Chinese Sellers Is Killing Small American Businesses*, FORBES (Feb. 14, 2017), https://www.forbes.com/sites/wadeshepard/2017/02/14/how-amazons-wooing-of-chinese-sellers-is-hurting-american-innovation/#13af78741df2.

[10] *See infra* Parts II.B & II.D.

[11] *See* Digital Millennium Copyright Act of 1998 (DMCA), 17 U.S.C. § 512 (Westlaw through Pub. L. No. 116-68) (creating a "safe harbor" from vicarious liability for ISPs that upon notification remove infringing material expeditiously). For cases holding that the ISP is not vicariously liable for the sale by third party vendors, s*ee generally Milo & Gabby, LLC v. Amazon.com, Inc.*, 2015 WL 4394673 (W.D. Wash. July 16, 2015); *Perfect 10, Inc. v. Amazon.com, Inc.*, 2009 WL 1334364 (C.D. Cal. May 12, 2009); *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003).

[12] *See infra* Parts II.B, II.D & II.E.

[13] *See* David Pierson, *Extra Inventory. More Sales. Lower Prices. How Counterfeits Benefit Amazon*, L.A. TIMES (Sept. 28, 2018), https://www.latimes.com/business/technology/la-fi-tn-amazon-counterfeits-20180928-story.html ("Not only has [Amazon] avoided any serious backlash for allowing the sale of fake goods, it's actually thrived from it, say more than two dozen brand owners, e-commerce consultants, attorneys, investigators and public policy experts.").

[14] *See infra* Parts II.D & II.E.

[15] *See* Pierson, *supra* note 13 ("[I]f Amazon shutters one store for selling knockoffs, the owner often shifts operations to another."); Alana Semuels, *Amazon May Have a Counterfeit Problem*, THE ATLANTIC (Apr. 20, 2018), https://www.theatlantic.com/technology/archive/2018/04/amazon-may-have-a-counterfeit-problem/558482/ ("'These problems come up once a week.'"). *Cf.* Jeff Bercovici, *Huge Counterfeiting Problem. This "Shark Tank" Company Is Fighting Back*, INC.COM (Apr. 2019), https://www.inc.com/magazine/201904/jeff-bercovici/amazon-fake-copycat-knockoff-products-small-business.html ("A recent Pointer report noted that Amazon in among the least responsive of all e-commerce platforms to takedown

MNCs have waged a decades-long struggle against Alibaba to stem the sale of counterfeits with few tangible results.[16] Although Alibaba claims to have made many serious efforts in combatting the sale of counterfeit goods, many brand owners remain frustrated and dissatisfied.[17] As in the case of Alibaba, brand owners in the United States are frustrated with what they perceive to be Amazon's half-hearted efforts to battle the flow of counterfeits.[18] This Article examines counterfeiting on the Internet with a focus on Alibaba and Amazon, the largest e-commerce platforms in China and the United States respectively and in the world.[19] The lessons learned can be immediately applied to other e-commerce platforms.

This Article focuses on why the sale of counterfeits on the Internet has exploded and allowed counterfeiters to penetrate markets that were previously unavailable when counterfeiters were limited to brick and mortar operations. Not only has the Internet given counterfeiters vast new opportunities for profit but it has also allowed them to operate in the digital world in the open, while simultaneously being able to use false cyber identities and addresses to evade detection and capture by brand owners and law enforcement authorities.[20] With the emergence of the Internet, counterfeiting and piracy—already a worldwide problem—have entered into a new and even more potent phase.[21] Up to the present, MNCs have been frustrated by their inability to curtail the growth of counterfeits on the Internet.[22]

Although the problems created by the Internet are daunting, this Article argues that a simple and effective deterrent exists in China but has been overlooked or ignored by MNCs and e-commerce platforms and explains how this deterrent can be used effectively. This Article sets forth for the first time how these remedial measures can be used to curtail the explosion of

notices, removing only 25 percent of infringing listings.").

[16] *See infra* Part II.D.

[17] *See id.*

[18] According to one brand owner representative, "Amazon is making money hand over fist from counterfeiters, and they've done about as little as possible for as long as possible to address the issue." Ari Levy, *Amazon's Chinese Counterfeit Problem Is Getting Worse*, CNBC (July 8, 2016), https://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html. *See also* Semuels, *supra* note 15 (describing Amazon's low level of responsiveness to brand owner concerns).

[19] Alibaba is the world's largest e-commerce marketplace and Amazon is the second largest. *See infra* notes 103 & 107.

[20] *See* Pierson, *supra* note 13.

[21] *See* BUS. ACTION TO STOP COUNTERFEITING AND PIRACY & INT'L CHAMBER OF COMMERCE, ROLES AND RESPONSIBILITIES OF INTERMEDIARIES: FIGHTING COUNTERFEITING AND PIRACY IN THE SUPPLY CHAIN 5 (2015), https://iccwbo.org/publication/roles-responsibilities-intermediaries/ ("The Internet has been particularly vulnerable . . . to counterfeiters and other criminal capitalizing on the success (and intellectual property) of legitimate businesses while remaining anonymous and avoiding detection.").

[22] *See infra* Part III.

counterfeits on the Internet. In setting forth this analysis, this Article will underscore the following three major points that must be understood by all MNCs and other brand owners in modern e-commerce. First, the emergence of e-commerce platforms such as Alibaba and Amazon have given counterfeiters a vast new tool to reach end use consumers. Prior to the Internet, counterfeiters were subject to the physical limitations created by brick-and-mortar distribution and retail sites and were unable to penetrate distribution channels that would allow them to sell counterfeits in reputable retail outlets.[23] Consumers had to travel to less desirable locations to buy counterfeits as state-owned department stores and high end retailers in China and large reputable retail chains such as Walmart, Target, and Costco in the United States refused to deal with distributors of counterfeit goods.[24] Instead, consumers in China or the United States who wished to purchase counterfeits had to go to small discount stores, mom-and-pop stores, flea markets, street vendors, or private addresses in side streets, back alleys or other undesirable locations, a prospect that deterred many consumers.[25] The emergence of the Internet has now given what counterfeiters have always sought: a legitimate distribution channel that consumers can access at any time from their computers without having to travel to undesirable locations to buy counterfeits from brick-and-mortar sellers.[26] The Internet also gives counterfeiters the ability to disguise their identities and to disappear into the vastness of cyberspace at the first sign of trouble.[27] All counterfeiters and pirates, whether they sell in brick-and-mortar locations or through the Internet, are very fearful of detection and capture.[28] Counterfeiters that use brick-and-mortar establishments are subject to surprise raids and seizures by enforcement authorities,[29] but Internet counterfeiters have found ways to use false identities that are untraceable by brand owners; even when they are detected, Internet pirates that are shut down are able to immediately create new false identities and return to their illegal operations on the Internet.[30]

Second, PRC enforcement officials have recently acknowledged in an

---

[23] *See* GAO REPORT, *supra* note 3, at 11.

[24] This observation is based on the author's own experience as an attorney working for U.S. brand owners in tracking the distribution channel of counterfeits.

[25] *Id. See* GAO REPORT, *supra* note 3, at 10 (counterfeits were traditionally sold in "underground" or secondary markets such as flea markets or sidewalk vendors).

[26] *See* GAO REPORT, *supra* note 3, at 11–12.

[27] *See id.*

[28] This observation is based on the author's firsthand experience in pursuing counterfeiters.

[29] *See* Chow, *supra* note 1, at 19 –21 (describing raids conducted in Yiwu City, "a significant wholesale distribution center for counterfeit goods in the PRC[,]" from 1998 to 1999).

[30] *See* Pierson, *supra* note 13 ("[B]rands say the same fraudsters keep showing up under different names[.]"); Semuels, *supra* note 15 ("Milo and Gabby tried to track down the [counterfeit] sellers, but almost all of the sellers had given false names when setting up their Amazon seller accounts, and the addresses they gave turned out to be bogus as well[.]").

official report that Alibaba sees itself as above the law in China and feels no need to follow it.[31] MNCs have long suspected that Alibaba tolerates or encourages counterfeiting on its sites.[32] Brand owners have persistently complained that Alibaba and Amazon appear reluctant to assist brand owners in tracking down counterfeiters and create unnecessary bureaucratic and technical hurdles in the detection of counterfeiters.[33] Some brand owners have attributed these difficulties to an economic motive: e-commerce platforms earn revenue through sales, including sales of counterfeit goods.[34] In the case of Alibaba, brand owners have long suspected that it tolerates or supports counterfeiting and these sentiments have been confirmed by official statements by PRC enforcement authorities. According to PRC officials, Alibaba's attitude towards the law and enforcement authorities is marked by a fundamental "arrogance."[35] In China, it is not unusual for powerful entities to view themselves as above the law.[36] The Communist Party, the most powerful entity of all, sees the law as a mere instrument to be used to serve the ends of the Party.[37] Alibaba is not intimidated by or fearful of law enforcement authorities; to the contrary, Alibaba sees itself as more powerful than government law enforcement authorities and answerable only to the Party.[38] For these reasons, MNCs must accept the reality that Alibaba, in the words of PRC officials, tolerates and supports counterfeiters in order to protect its revenues from sales of counterfeit goods and that it will likely take an intervention by the Party at its highest levels to effect meaningful change in Alibaba's conduct. Any plan to stem the sales of counterfeits on Alibaba's platform that requires Alibaba's active participation must proceed with the assumption that it will be met with resistance or efforts that are half-hearted.

Third, although the use of the Internet to sell counterfeits presents formidable new challenges to brand owners, this Article argues that simple and effective measures are available under PRC law to brand owners to deter

---

[31] *See* Gongshang Zongju (工商总局), Guanyu Dui Alibaba Jituan Jinxing Xingzheng Zhidao Gongzuo Qingkuang de Baipishu (关于对阿里巴巴集团进行行政指导工作情况的白皮书), *translated in* STATE ADMIN. OF INDUS. & E-COMMERCE, PEOPLE'S REPUBLIC OF CHINA, WHITE PAPER ON ALIBABA GROUP HOLDINGS ADMINISTRATIVE GUIDANCE WORK SITUATION (2015) [hereinafter SAIC WHITE PAPER]. A partial English translation is available at Zheping Huang, *The Chinese Government Has Erased a Damning Report on Alibaba, but You Can Read It Here*, QUARTZ (Jan. 29, 2015), https://qz.com/335675/the-chinese-government-has-erased-a-damning-report-on-alibaba-but-you-can-read-it-here/. The SAIC White Paper is extensively discussed in Part II.B.

[32] *See infra* Part II.B.

[33] *See infra* Part III.A.

[34] *See e.g.*, Pierson, *supra* note 13 ("Not only has [Amazon] avoided any serious backlash for allowing the sale of fake goods, it's actually thrived from it, say more than two dozen brand owners, e-commerce consultants, attorneys, investigators and public policy experts.").

[35] SAIC WHITE PAPER, *supra* note 31, at 20.

[36] *See infra* Part II.D.2.b.

[37] *Id.*

[38] *Id.*

many counterfeiters from using the Internet and to detect and identify those that do.[39] This Article proposes and sets forth for the first time a set of simple and effective methods that MNCs can use to create effective deterrence to counterfeiting on the Internet.[40] To the best of the author's knowledge, no MNC, brand owner, or any professional or academic study has previously identified these methods, although they are openly available in plain sight in China's legal system, and their use is required and regularly encouraged by PRC officials. Although certain aspects of China's information technology industry, such as protection and enforcement of intellectual rights, are weak by comparison to the United States, other aspects of China's information technology industry are far ahead of the United States.[41] In particular, China's obsessive need to exert pervasive control over and to monitor its citizens and all aspects of Chinese society have created the informational technology tools available to deter counterfeiters.[42] In fact, Chinese government officials have urged Internet sites to use the tools available to control entry onto Internet sites and to monitor entities on the Internet.[43] Brand owners, however, either do not trust PRC officials or understand the potential effectiveness of these tools.

Unlike brick-and-mortar counterfeiters who need no permission to operate, counterfeiters must obtain a "pass" through a digital port of entry in order to obtain access to the Internet to sell their products.[44] Operators of e-commerce platforms have the ability to exercise absolute control over entry. Controlling this point of entry through the use of tools created by the PRC government is the key to controlling counterfeiting on the Internet. Counterfeiters wish to operate in hiding and secrecy; they fear and detest transparency and accountability. E-commerce platforms can remove the anonymity of the Internet by following a straightforward registration system

---

[39] *See infra* Part III.

[40] *Id.*

[41] China is far ahead of the U.S. in the use of technologies, such as facial recognition, to closely monitor its citizens. *See* Zhou Jiaquan, *Drones, Facial Recognition, and a Social Credit System: 10 Ways China Monitors Its Citizens*, S. CHINA MORNING POST (Aug. 4, 2018), https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china.

[42] China closely monitors its citizens. Recently, China announced a "social credit" system in which the activities of each citizen will be ranked, and each citizen given a score evaluating the social merit of his or conduct. For a discussion on how China monitors its citizens, *see* Charlie Campbell, *How China Is Using "Social Credit Scores" to Rewards and Punish Its Citizens*, TIME (Jan. 16, 2019), https://time.com/collection/davos-2019/5502592/china-social-credit-score/.

[43] *See infra* Part III.

[44] Online vendors are required by e-commerce platforms to register before they are allowed to access the site. *See e.g.*, *Selling on Amazon: Frequently Asked Questions*, AMAZON, https://services.amazon.com/selling/faq.htm (last visited July 1, 2019) (requiring a business name, address, and contact information among other information in order to open an Amazon seller account).

as required by PRC law.[45] However, Alibaba does not faithfully apply the requirements of PRC law but instead is careless and loose in verifying entity registration.[46] Brand owners also complain that Amazon has lax registration requirements and registers many entities with fictitious identities and addresses.[47]

As a condition of gaining access to e-commerce sites, PRC law requires all vendors to submit a business license issued by PRC government authorities. These licenses have strict disclosure requirements that will reveal their true legal identities and locations in strict accordance with the detailed and specific information contained in official PRC government records and electronically on government websites to the public.[48] To obtain this official business license, business operators must undergo a review and approval process by PRC government authorities over the legality and economic feasibility of their proposed business operations.[49] Most counterfeiters will not wish to submit to such an approval process for fear of being detected and being subject to capture and prosecution. Those entities that do undergo this official review will then need to openly display their business licenses on the website In turn, counterfeiters will be unable to escape detection as brand owners will be able to bring suit directly against them.[50]

A unique concept of PRC law is that each business entity must have a natural person who serves as its legal representative and who is subject to civil liability and criminal prosecution.[51] The legal representative must be identified in the business license so brand owners will have a person in flesh and blood against whom they can directly file civil or criminal actions in China or in the United States if U.S. contacts exist.[52] The faithful execution of these requirements should help brand owners to deter many counterfeiters from selling through Internet sites. Currently, however, brand owners do not insist on enforcement of these requirements and neither Alibaba nor Amazon faithfully follows PRC law on entity registration.[53]

This Article will proceed as follows. Part II examines the background

---

[45] *See infra* Part III.

[46] *See* text accompanying notes *231-34 infra.*

[47] *See infra* note 95.

[48] *See* Administrative Measures for Online Trading, art. 23 (promulgated by the State Admin. of Indus. & E-Commerce, Order No. 60, Jan. 26, 2014, effective Mar. 15, 2014), CLI.4.218557(EN), http://en.pkulaw.cn/display.aspx?id=16309&lib=law&EncodingName=big5. *See also infra* Part III.

[49] *See infra* Part III.

[50] *Id.*

[51] *See* General Principles of the Civil Law of the People's Republic of China, ch. III, art. 57 (promulgated by the Nat'l People's Cong., Order No. 66, Mar. 15, 2017, effective Oct. 1, 2017), *translated by* Whitmore Gray & Henry Ruiheng Zheng, *General Principles of the Civil Law of the People's Republic of China*, 34 AM. J. COMP. L. 715, 726 (1986) [hereinafter General Principles of the Civil Law of the PRC].

[52] *See infra* Part III.

[53] *Id.*

of counterfeiting in China and how the advent of the Internet has propelled this illegal activity to new heights. The ability to transcend the physical limitations created by brick-and-mortar counterfeiting operations has created a vast new opportunity in cyberspace for counterfeiters who can now compete directly with genuine goods and vanish at the first sign of trouble. Part II also discusses brand owner concerns about Alibaba and Amazon. In the case of Alibaba, brand owners have long claimed that Alibaba tolerates or supports counterfeiting on its websites. A recent in-depth investigation and report by PRC national authorities not only confirms this suspicion but also sets forth the PRC government's view that Alibaba sees itself as being above the law. Brand owners have also complained that Amazon is unresponsive to their concerns about counterfeits, requiring byzantine notice and takedown procedures that only add to brand owners' misery. Part III examines the hurdles that brand owners claim that they face in attempting to work with Alibaba and Amazon in removing infringing webpages or postings from their sites; these frustrations are due to cumbersome notice and takedown procedures that can take months and tax brand owners through heavy costs in time, energy, and money. Part III then sets forth this Article's proposed method of using existing online tools in the PRC to help create deterrents to counterfeiting on the Internet. These tools can be used to combat counterfeits on Alibaba and Amazon as well as on other e-commerce platforms. Part IV contains concluding observations.

II. COUNTERFEITING AND THE INTERNET

A. Brief Overview of Counterfeiting in China

As early as 2000, China was described as having the most serious counterfeiting problem in world history.[54] The origin of this problem can be traced to 1) China's access to advanced technology (i.e. intellectual property) brought into China by MNCs that make foreign direct investments in China and 2) to China's weak and developing legal system,[55] which does not create effective deterrence for counterfeiters and infringers of intellectual property rights.[56] Although U.S. companies have made many efforts through the first two decades of the twenty-first century to combat counterfeiting in China, China remains the largest source of counterfeits in the world. For example, a recent study cited in Forbes indicates that China produces 80% of the world's counterfeits and that counterfeiting is now a $1.7 trillion per year industry.[57]

[54] Chow, *supra* note 1, at 3. The background and history of the rise of counterfeiting before the advent of the internet is set forth in this article. *See infra* Parts II.A & II.B.

[55] DANIEL C.K. CHOW & THOMAS J. SCHOENBAUM, INTERNATIONAL BUSINESS TRANSACTIONS 537–38 (3d. ed. 2015).

[56] DANIEL C.K. CHOW & THOMAS J. SCHOENBAUM, INTERNATIONAL TRADE LAW 643 (3d. ed. 2017) (China's weak legal system does not create effective deterrence.).

[57] Wade Shepard, *Meet the Man Fighting America's Trade War Against Chinese Counterfeits (It's Not Trump)*, FORBES (Mar. 29, 2018), https://www.forbes.com/sites/wade

The U.S. General Accountability Office reports that in 2016, 88% of all seized counterfeit goods by the United States originated from China and Hong Kong.[58] The European Union claims that China is the largest source of counterfeit goods sold into the EU.[59] Counterfeiting is now the largest criminal enterprise in the world,[60] and China is the epicenter of counterfeiting.[61] The highest number of shipments of counterfeits seized around the world originates from East Asia, with China as the top source.[62]

On April 3, 2019, the Trump Administration issued a Presidential Memorandum announcing that combatting counterfeiting and piracy had been elevated to a new level of priority for the United States.[63] The memorandum specifically tasked the Justice Department and the Department of Homeland Security to focus on and investigate "online third party marketplaces."[64] This indicates a recognition by the United States that counterfeiting on e-commerce platforms is a specialized priority area of concern.

B. The Advent of the Internet

The rise of Internet sales platforms in the early 2000s created a valuable new opportunity for counterfeiters. To understand the significance of this development, it is necessary to recognize that there are two main components to counterfeiting: manufacturing and distribution.[65]

The manufacturing of counterfeits tends to arise in proximity to the manufacturing of genuine goods.[66] In the early 1990s, one of the first areas open to foreign investment in China was in the southern region of Guangdong Province, near Hong Kong. MNCs opened manufacturing facilities in special

shepard/2018/03/29/meet-the-man-fighting-americas-trade-war-against-chinese-counterfeits/#321a1941c0d6.

[58] GAO REPORT, *supra* note 3, at 13.

[59] EUROPEAN COMM'N, EU SEIZURES AT THE BORDER OF GOODS INFRINGING ON INTELLECTUAL PROPERTY RIGHTS (2018), https://ec.europa.eu/taxation_customs/sites/taxation/files/factsheet_ipr_report_2018_en.pdf.

[60] *See* Shepard, *supra* note 57 ("The trade in counterfeit and pirated goods is currently at $1.7 trillion . . . and is expected to grow to $2.8 trillion and cost 5.4 million jobs by 2022.").

[61] *See id. See also* EUROPEAN COMM'N, *supra* note 59 (reporting that China and Hong Kong, together, accounted for over 83% of counterfeit goods).

[62] OECD & EUROPEAN UNION INTELLECTUAL PROP. OFFICE, TRADE IN COUNTERFEIT AND PIRATED GOODS: MAPPING THE ECONOMIC IMPACT 49 (2016), http://dx.doi.org/10.1787/9789264252653-en.

[63] Memorandum on Combatting Trafficking in Counterfeit and Pirated Goods, Section 1 (Apr. 3, 2019), https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/.

[64] *Id.*

[65] Daniel C.K. Chow, *Organized Crime, Local Protectionism and the Trade in Counterfeit Goods in China*, 14 CHINA ECON. REV. 473, 474 (2003).

[66] *Id.*

economic zones that created financial incentives for investment.[67] Soon after these facilities were established, the brand owners found that counterfeits began to appear in the same locations.[68] MNCs discovered that employees working in their facilities or their relatives, friends, or associates had begun to use the know-how that they acquired from the MNC to establish their own manufacturing operations in order to produce counterfeits.[69]

A counterfeiter that has manufactured a fake good must then sell it to consumers. The illegal factory may be located far away from densely populated urban areas where large numbers of consumers are found, so the counterfeiter must find a distribution channel for the goods to reach the end-use consumer. Distribution is the second major component of counterfeiting.

Prior to the rise of the Internet, counterfeiters faced a problem: legitimate distributors would have nothing to do with counterfeits.[70] MNCs distribute their products in China only through qualified distributors that are able to sell to high-end state-owned department stores and other retail outlets in high-end shopping centers.[71] Qualified distributors are those entities that are able to pass a stringent set of criteria established by brand owners.[72] These distributors will not work with counterfeiters for fear of losing their contracts with legitimate brand owners, and, as a result, counterfeiters are unable to penetrate into legitimate distribution channels to reach high-end retailers.[73] Rather, counterfeiters had to rely on brick-and-mortar wholesale distributors of lesser and questionable repute who would be willing to sell counterfeits, smuggled goods, and inferior quality products.[74] These wholesale distributors are found in markets in China that are either enclosed or open air spaces with hundreds or thousands of wholesale vendors.[75] Retailers appear at these wholesale markets with trucks or vans to transport the counterfeits purchased at these markets.[76] Large reputable retailers, such as state-owned department stores, do not buy at these wholesale markets.[77] Only retailers that are small mom and pop stores, street stalls, or open air vendors in China will purchase from these markets.[78] This left the counterfeiter with the problem that it could

---

67 *Id.*

68 *See id.* at 474–75.

69 This observation is based upon the author's own experience working as in-house counsel for an MNC with major operations in China. It is a pattern that is repeatedly occurs in China: counterfeiting tends to arise in locations with legitimate manufacturing operations.

70 *See* Chow, *supra* note 65, at 476.

71 *Id.*

72 *Id.*

73 *Id.*

74 *See id.* at 476–77.

75 *Id.* at 476.

76 *See* Chow, *supra* note 65, at 476.

77 *Id.*

78 *Id.*

almost never penetrate into high-end retail stores.[79] Purchasers of counterfeits would have to travel to side streets, back alleys, and other areas in less desirable urban locations to buy counterfeits from small and less reputable retailers.[80] The need to travel to unsavory locations deterred many consumers.

In the United States, counterfeits are also unable to penetrate into legitimate distribution channels to reach large department stores or other large retailers.[81] Counterfeits are almost never found in large chain stores such as Costco, Target, or Walmart. These companies either use qualified distributors or have vertically integrated business models that allow them to control distribution themselves.[82] These distributors refuse to deal in counterfeits, smuggled goods, or gray market goods.[83] Only less reputable distributors will deal in these secondary goods, but they do not sell to large and high end retailers who refuse to deal with them.[84] These distributors sell to discount stores, small mom-and-pop stores, street vendors, or private persons who arrange for sales through word of mouth.[85]The advent of the Internet has now given counterfeiters what they have long sought: a legitimate and broad-reaching distribution channel to reach retail consumers who are now able to purchase products without having to travel to specific and undesirable locations where counterfeits are sold. Counterfeiters can now place their products on the Internet to reach consumers worldwide and are no longer confined to using illegal wholesale markets to reach lower retail quality stores. While in the past, consumers would not encounter counterfeits on the next shelf adjacent to authentic goods in brick and mortar stores because high end retailers refused to deal with distributors of counterfeit goods, the same is no longer true on the Internet. It is now possible for counterfeits to be on the digital shelf next to genuine goods on the same or an adjacent webpage.[86] Counterfeits can now compete directly with genuine goods.[87] Counterfeiters can also use false digital images that hide the low

---

[79] *Id.*

[80] *Id.*

[81] This observation is based on the author's own experience as an expert witness in U.S. litigation involving U.S. multinational companies in cases involving counterfeits from China.

[82] *Id.*

[83] Gray market goods (sometimes also called parallel imports) are genuine goods that are intended for sale in a foreign market but that are purchased abroad and shipped back to the home market. For example, genuine goods that are sold by the manufacturer to Japan are purchased by a foreign distributor in Japan who then resells them to an importer in China. The foreign distributor is able to take advantage of a lower price in Japan or favorable currency exchange rates in order to sell the products in China at a price that is lower than the genuine goods are sold directly by the manufacturer to buyers in China. See CHOW & SCHOENBAUM, *supra* note 55, at 567-68.

[84] *See* Chow, *supra* note 65, at 476.

[85] *Id.*

[86] *See* GAO REPORT, *supra* note 3, at 11.

[87] *Id.* ("In the past, consumers could often rely on indicators such as appearance, price, or

quality of their goods in competition with genuine goods.[88]

The rise of counterfeits coincides with shifts in consumer habits. In June 2000, approximately 22% of U.S. consumers purchased goods online, but by December 2016 that portion had risen to 79%.[89] By 2020, worldwide e-commerce sales are expected to reach $4 trillion, and e-commerce is expected to reach nearly 15% of global retail spending by 2020.[90]

Prior to the advent of the Internet, counterfeiters in China that sought to sell their goods in the United States loaded the goods in large shipping containers with false documentation to transport the goods by ocean carriage to a port in the United States.[91] While detection was difficult, if a brand owner had reliable specific intelligence of an illegal shipment,[92] customs authorities in the United States would open and inspect the container.[93] With Internet sales, thousands or hundreds of thousands of small, individual packages are now shipped to the United States by mail, making it nearly impossible to detect and stop these shipments.[94]

Not only do e-commerce platforms allow counterfeiters unprecedented access to end use consumers, counterfeiters are also able to take advantage of the anonymity of the internet to evade capture and detection by using false identities, business names, and locations.[95] The Internet has created an irresistible new opportunity for counterfeiters and has opened vast new avenues for generating profit.

C. Liability Regimes for Internet Service Providers

Under the Digital Millennium Copyright Act (DMCA)[96] in the United

---

location of sale to identify counterfeit goods in the marketplace, but counterfeiters have adopted new ways to deceive customers.").

88 *Id. Cf. id.* ("The physical appearance of counterfeit goods may no longer serve as a 'red flag' for consumers that the good they are considering purchasing is not genuine. Counterfeit goods and their packaging are becoming more sophisticated and closely resemble genuine goods[.]").

89 *Id.* at 12.

90 *Id.*

91 *See* Chow, *supra* note 65, at 475.

92 Such intelligence can be gathered through the use of private investigation companies that penetrate counterfeit rings. A number of companies, such as Kroll and Pinkerton, specialized in these investigations.

93 The author was involved as an attorney in a counterfeiting case in the United States in which U.S. Customs authorities stated that they would be willing to conduct an inspection of shipping containers but only on the basis of reliable specific information.

94 *See* Pierson, *supra* note 13 ("Customs agents had a fighting chance when pirated goods predominantly arrived in cargo containers. But with the rise of e-commerce, counterfeiters and their middlemen can ship goods in parcels too innumerable to catch.").

95 *See id.* ("[B]rands say the same fraudsters keep showing up under different names[.]"); Semuels, *supra* note 15 ("Milo and Gabby tried to track down the [counterfeit] sellers, but almost all of the sellers had given false names when setting up their Amazon seller accounts, and the addresses they gave turned out to be bogus as well[.]").

96 17 U.S.C. § 512 (Westlaw through Pub. L. No. 116-68). DMCA implements two World

States and similar provisions in China,[97] Internet service providers (ISPs) are not directly liable for the sale of counterfeits listed on their sites by third-party vendors.[98] While ISPs may be subject to vicarious liability for facilitating the sales, DCMA provides a "safe harbor."[99] ISPs are entitled to immunity from vicarious liability for third-party listings and sales of counterfeit goods if they have no knowledge of the infringing material and remove it expeditiously upon receiving notice of its illegal nature.[100] To implement DCMA and the corresponding PRC law, e-commerce companies such as Alibaba and Amazon have set forth internal notice and takedown procedures that brand owners are required to follow when they find infringing material.[101] As detailed in a later section, brand owners often complain that these procedures are cumbersome, time consuming, and ineffective.[102]

D. Alibaba

1. Brand Owner Concerns

Alibaba is currently the world's largest e-commerce platform in the world.[103] In 2016, Alibaba's Internet marketplaces in China had 423 million

---

Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. WIPO Copyright Treaty, Dec. 20, 1996, 112 Stat. 2861, 2186 U.N.T.S. 121; WIPO Performances and Phonograms Treaty, Dec. 20, 1996, 112 Stat. 2861, 2186 U.N.T.S. 203. As of 2007, the United States and the People's Republic of China are now contracting parties to both treaties. *Contracting Parties – WIPO Copyright Treaty*, WIPO, https://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16 (last visited July 1, 2019); *Contracting Parties – WIPO Performances and Phonograms Treaty*, WIPO, https://www.wipo.int/treaties/en/ShowResults.jsp? lang=en&treaty_id=20 (last visited July 1, 2019).

[97] *See generally* Trademark Law of the People's Republic of China (promulgated by the Nat'l People's Cong., adopted Aug. 23, 1982, most recently revised Apr. 23, 2019, effective Nov. 1, 2019); Law Against Unfair Competition of the People's Republic of China (promulgated by the Nat'l People's Cong., Order No. 10, Sept. 2, 1993, revised Nov. 4, 2017, amended Apr. 23, 2019).

[98] *See* 17 U.S.C. § 512(c)(1).

[99] *Id. See generally* Susanna Monseau, *Fostering Web 2.0 Innovation: The Role of the Judicial Interpretation of the DMCA Safe Harbor, Secondary Liability and Fair Use*, 12 J. MARSHALL REV. INTELL. PROP. L. 70 (2012).

[100] *See* 17 U.S.C. § 512(c)(1).

[101] *See Intellectual Property Policy for Sellers*, AMAZON, https://sellercentral.amazon.com/gp/help/external/201361070 (last visited July 1, 2019); *Intellectual Property Rights (IPR) Protection Policy*, ALIBABA, https://rule.alibaba.com/ rule/detail/2049.htm (last visited July 1, 2019).

[102] *See infra* Part III.

[103] Comment Submitted by Eric Pelletier, Vice President of Alibaba, to the Honorable Probir Mehta, Assistant United States Trade Representative re: 2016 Special 301 Out-of-Cycle Review Notorious Markets (Docket Number USTR-2016-2013), at 2 (Oct. 7, 2016), https://www.alizila.com/wp-content/uploads/2016/10/P-Alibaba-Group-Comments-for-2016-Notorious-Markets-Report-2_FINAL_compressed.pdf?x95431 (last visited Nov. 25,

active purchasers with a combined gross merchandise volume (GMV) of $485 billion.[104] In 2018, in the span of just two years, active purchasers in China grew to 636 million and GMV grew to exceed $768 billion,[105] creating the prospect that Alibaba's users may soon surpass one billion and its GMV may soon surpass $1 trillion, numbers that seemed almost inconceivable just a decade ago. In 2015, package delivery from Alibaba's e-commerce platform in China averaged thirty million per day.[106] The sheer size and scope of Alibaba's operations dwarfs even that of its closest competitors. For example, Alibaba's GMV in 2018 at $768 billion is more than three times that of Amazon, the world's second e-commerce platform, at $239 billion.[107]

From Alibaba's earliest days of operation, back in 1999, MNCs have claimed that counterfeits are abundantly available on Alibaba's websites.[108] Frustrated with the lack of results in China, U.S. companies have raised these concerns with the U.S. government and, as a result, Alibaba has been repeatedly placed on U.S. government blacklists. Despite its many claims that it is implementing new changes to effectively combat counterfeiting on its websites, Alibaba was first placed on the Out-of-Cycle Notorious Markets List in 2011[109] and sought to remove itself from the list in anticipation of its initial public offering (IPO) in the United States in 2014. Although Alibaba was dropped from the 2012 list,[110] Alibaba found itself once again on the

2019).

[104] *Id.*

[105] Press Release, Alibaba Group Announces December Quarter 2018 Results (Jan. 30, 2019), https://www.alibabagroup.com/en/news/press_pdf/p190130.pdf.

[106] Jen Wieczner, *Alibaba: Here's Why Our Mind-Blowing Numbers Are Real*, FORTUNE (Sept. 23, 2015), https://fortune.com/2015/09/23/alibaba-says-numbers-real-not-fake/.

[107] Adam Levy, *The 7 Largest E-Commerce Companies in the World*, THE MOTLEY FOOL (Dec. 26, 2018), https://www.fool.com/investing/2018/12/26/the-7-largest-e-commerce-companies-in-the-world.aspx.

[108] *See, e.g.*, *Alibaba and the 2,236 Thieves: An Online-Fraud Scandal in China*, THE ECONOMIST (Feb. 22, 2011), https://www.economist.com/newsbook/2011/02/22/alibaba-and-the-2236-thieves;

[109] OFFICE OF U.S. TRADE REPRESENTATIVE, 2011 OUT-OF-CYCLE REVIEW OF NOTORIOUS MARKETS 3 (Dec. 20, 2011), https://ustr.gov/sites/default/files/uploads/gsp/speeches/reports/2011/Notorious%20Markets%20List%20 FINAL.pdf (discussing Alibaba's subsidiary site Taobao.com).

[110] Doug Palmer, *U.S. Drops China's Taobao Website from "Notorious" List*, REUTERS (Dec. 13, 2012), https://www.reuters.com/article/net-us-usa-trade-piracy/u-s-drops-chinas-taobao-website-from-notorious-list-idUSBRE8BC1IG20121213.

Notorious Markets list in 2014[111], 2016[112], 2017[113], and 2018[114]. Furthermore, in 2016, a group of 17 international trade associations reiterated their concerns in a letter to USTR, stating:

> During the ten months since USTR published [the 2015 USTR Special 301 Notorious Markets Report] we have seen little evidence that there has been any noticeable change on the Alibaba platforms themselves; and at any given moment, a consumer around the world can chose from hundreds of thousands of counterfeit clothes, shoes, travel goods, handbags, toys, auto parts, jewelry, watches, furniture, electronics, pharmaceuticals, and other articles.[115]

Many brand owners have concluded that Alibaba, despite its protestations to the contrary, actually tolerates and supports counterfeiting on its websites because Alibaba earns revenues from all sales, including sales of counterfeit goods. Labelling Alibaba as "our most dangerous and damaging adversary,"[116] one brand owner stated:

> Alibaba's strategy has consistently been to provide lip service to supporting brand enforcement efforts while doing as little as possible to impede the massive flow of counterfeit merchandise on its platforms.[117]

---

[111] OFFICE OF U.S. TRADE REPRESENTATIVE, 2014 OUT-OF-CYCLE NOTORIOUS MARKETS LIST 8 (Mar. 5, 2015), https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published_0.pdf (discussing Alibaba's subsidiary site Taobao.com).

[112] OFFICE OF U.S. TRADE REPRESENTATIVE, 2016 OUT-OF-CYCLE NOTORIOUS MARKETS LIST 12–13 (Dec. 2016), https://ustr.gov/sites/default/files/2016-Out-of-Cycle-Review-Notorious-Markets.pdf (discussing Alibaba's subsidiary site Taobao.com).

[113] OFFICE OF U.S. TRADE REPRESENTATIVE, 2017 OUT-OF-CYCLE NOTORIOUS MARKETS LIST 20–23 (Jan. 11, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2017%20Notorious%20Markets%20List%201.11.1 8.pdf (discussing Alibaba's subsidiary site Taobao.com).

[114] OFFICE OF U.S. TRADE REPRESENTATIVE, 2018 OUT-OF-CYCLE NOTORIOUS MARKETS LIST 26–27 (Jan. 11, 2018), https://ustr.gov/sites/default/files/2018_Notorious Markets_List.pdf (discussing Alibaba's subsidiary site Taobao.com).

[115] Comment Submitted AFL-CIO et al. to the Honorable Probir Mehta, Assistant United States Trade Representative re: 2016 Special 301 Out-of-Cycle Review Notorious Markets (Docket Number USTR-2016-2013), at 2 (Oct. 26, 2016), https://www.mema.org/sites/default/files/resource/Multi-Org%20Letter%20on%20Alibaba%20102616.pdf.

[116] Letter from Lee S. Sporn of Michael Kors (USA), Inc. to Bob Barchiesi, President, International Anti-Counterfeit Coalition (IACC), at 2 (Apr. 21, 2016) [Hereinafter Letter from Lee S. Sporn]. *See* Erika Kinetz, *Some Howl Over Alibaba's Place in Anti-Counterfeiting Group*, ASSOC. PRESS (May 5, 2016), https://www.apnews.com/2c9381cb0c2841aba956abef1a3005b3.

[117] Letter from Lee S. Sporn, *supra* note 116, at 2. *See* Kathy Chu, *Brands Voice Doubts After Alibaba Joins Group Fighting Fake Goods*, WALL ST. J. (Apr. 28, 2016), https://www.wsj.com/articles/brands-voice-doubts-after-alibaba-joins-group-fighting-fake-goods-1461763178.

a. Alibaba's Defense of Counterfeits

Many brand owners' skepticism about Alibaba's sincerity in combatting counterfeiting can be attributed to statements made by its Chairman and founder, Jack Ma, that defend counterfeiting. In responding to criticism by luxury brands about the sale of counterfeits on Alibaba, Ma made clear his position in 2015. A commentator observed:

> The longer Ma talks, the more it's clear where his sentiments fall. The second-richest man in China thinks the very idea of luxury retail—selling belts and accessories and the like for thousands of dollars—is inherently absurd. "How can you sell Gucci or whatever branded bag for so much money? It is ridiculous," he says. "I understand the branded companies are not happy, but I also say that's your business model. You have to check your business model, too."[118]

The following year, in a speech at Alibaba's headquarters, Ma stated:

> The problem is the fake products today are of better quality and better price than the real names. They are exactly the [same] factories, exactly the same raw materials but they do not use the names.[119]

These statements suggest that Ma believes that there is a normative justification for Alibaba's support of counterfeits. Ma believes luxury brands like Gucci are inviting unauthorized copies by charging prices so high that they are "absurd." Alibaba sees itself as helping out small-time sellers that sell counterfeits or infringing products to lift themselves into the middle class. Jack Ma and Alibaba take on a modern "Robin Hood" persona. Just as the fictional Robin Hood robbed from the rich to give to the poor, Alibaba is assisting small-time Chinese sellers to take a free ride on the goodwill of luxury brands owned by MNCs that have invited counterfeiting through their greed, avarice, and attempts to gouge vulnerable Chinese consumers. China's consumers also benefit from having access to fakes that are "of better quality and better price than thee real names."[120] Ma's position may help Alibaba to further gain popularity in China by enhancing Ma's reputation as a true national hero and great patriot of China, but it also infuriates brand owners.[121]

---

[118] Michael Schuman, *Why Alibaba's Massive Counterfeit Problem Will Never Be Solved*, FORBES (Nov. 4, 2015), https://www.forbes.com/sites/michaelschuman/2015/11/04/alibaba-and-the-40000-thieves/#31848fd729dc.

[119] Charles Clover, *Alibaba's Jack Ma Says Fakes Are Better Than Originals*, FIN. TIMES (June 14, 2016), https://www.ft.com/content/6700d5cc-3209-11e6-ad39-3fee5ffe5b5b.

[120] *Id.*

[121] *See* Letter from Lee S. Sporn, *supra* note 116. When Alibaba was accepted as a member of the International Anti-Counterfeiting Coalition, Sporn, who represents Michael Kors, a fashion house, resigned in protest. Chu, *supra* note 117.

b. Counterfeits for Sale on Alibaba

To test the claims of brand owners that counterfeits are found in abundance on Alibaba's sites, the author recently did a search of Alibaba sites and immediately found many examples of counterfeits and infringing products. Photographs of the webpages containing three of these examples are set forth in the Appendices. These examples are discussed below, but there are other examples on this site that are too numerous to discuss within the confines of this Article.

(a) Appendix 1 is an advertisement for handbags being sold under a "big brand name" ("Da Pai") called "Gucci Guccio." These handbags copy the design and trade dress of Gucci handbags and use the name "Gucci" as part of their brand name.[122] Gucci was singled out by Alibaba Chairman Jack Ma as a luxury brand owner selling its products at absurdly high prices.[123] The advertised price for these products is 1500 Renminbi ("people's currency" or RMB, the Chinese fiat currency). At the currency exchange rate of 1 RMB to 0.15 U.S. dollar, this price is the equivalent of about $225 U.S. dollars. On Gucci's website in the United States, genuine Gucci bags similar to the ones advertised on Alibaba sell for over $2000 U.S. dollars with some bags selling for as much as $7500.[124] It is highly unlikely for a genuine Gucci handbag of the type in this advertisement to sell for $225. It is also highly unlikely that these types of prices can be charged for gray market goods.[125] In addition, nothing in the advertisement indicates that these are second hand or used goods. Chinese consumers have an aversion to purchasing secondhand goods due to cultural reasons, and Chinese merchants are well aware of consumers' dislike of secondhand goods.[126] It is highly likely that the products advertised in the attached Alibaba webpage are counterfeits.

(b) Appendix 2 is an advertisement for a 700 ml bottle of Hennessy

[122] The author was told by an associate in China that Alibaba did not consider "Gucci Guccio" to be an infringing or counterfeit use because the name "Gucci" did not appear alone but was accompanied or modified by another name as part of the product's brand name. Only the unauthorized use of a trademark such as Gucci appears alone would be considered an infringing use.

[123] *See infra* text accompany note 117.

[124] *Women's Handbags*, GUCCI, https://www.gucci.com/us/en/ca/women/womens-handbags-c-women-handbags/1 (last visited July 1, 2019).

[125] While prices for gray market goods are usually lower than prices for genuine goods intended for the home market, the price differential would not be as great as that set forth in the case of the handbags in Appendix 1, i.e. it would be highly unlikely that a genuine handbag that sold for approximately $2,000 to $7,500 in Japan could be sold as a gray market good in China for $225. CHOW & SCHOENBAUM, *supra* note 55, at 567.

[126] *See* Yiling Pan, *Why the Second Hand Luxury Market isn't Thriving in China*, JING DAILY (Aug. 24, 2017), https://jingdaily.com/what-blocks-secondhand-luxury-market-thriving-in-china/ (last visited July 12 2019) (Chinese consumers "still prefer to purchase new luxury goods and look down on the value of second-hand goods").

> XO cognac with an advertised price of 432 RMB or $65. A similarly sized bottle (750 ml) sells for approximately $160 in the United States.[127] It is highly likely that the bottle sold on the Alibaba website is a counterfeit.
>
> (c) Appendix 3 is an advertisement for fashion workout pants made by Abercrombie and Fitch, based in Columbus, Ohio, selling at a price of 80 RMB or $12. Based on the photograph and the author's experience in tracking counterfeiters in the consumer products industry, it is apparent that these products are of low quality and are inferior to what Abercrombie and Fitch would sell in retail stores. By comparison, Appendix 4 includes a photograph of a similar Abercrombie and Fitch product from its website that sells for $58.[128] These facts indicate that it is highly likely that the product advertised on the Alibaba website is a counterfeit.

To understand why brand owners view examples such as these as threats to their business, it is necessary to realize that in China (as in many other countries) there is a huge appetite for counterfeit goods, and many consumers actively search for and buy counterfeits.[129] The vast majority of consumers in China who visit the webpages for the products described in the examples above are fully aware that these are counterfeit goods, but these consumers are actively seeking these goods.[130] In the case of counterfeit Gucci handbags and counterfeits of other famous brand names, consumers are actively seeking to buy cheap imitations of the famous brand that they can purchase for a tenth or less than the genuine product.[131] These consumers want the prestige of the brand, trademark, or trade dress and are not concerned about the quality of the actual merchandise itself.[132] So long as the product has the trademark or trade dress, the purchaser of the counterfeit is able to enjoy the

---

[127] *Hennessy Cognac XO*, WINE CHATEAU, https://www.winechateau.com/products/hennessy-cognac-xo (last visited July 1, 2019).

[128] *See* Appendix 4 *infra*.

[129] Jay Kennedy, *Commentary: More Buying Counterfeits and Knockoff - It's Costing Billions and More* (May 12, 2019), CHANNEL NEWS ASIA, https://www.channelnewsasia.com/news/commentary/more-buy-knock-off-counterfeit-fake-goods-branded-drug-crime-11499382 (noting that "there are many consumers who willingly buy counterfeit goods"). *See also The Counterfeit Goods Industry in Modern China* (April 15, 2019), DAXUE CONSULTING, https://daxueconsulting.com/counterfeit-products-in-china/ (noting that "the market for fake goods in China is largely driven by consumers who actively search for and purchase counterfeit products").

[130] This observation is based on the author's own experience in China. *See* Liz Robbins, Investigators Seize Fake Luxury Goods, N.Y. TIMES (Aug. 16, 2018), https://www.nytimes.com/2018/08/16/nyregion/fake-luxury-goods-handbags.html.

[131] This observation is based on the author's work with private investigation companies tracking counterfeiters in China.

[132] *See* DANIEL C.K. CHOW & EDWARD LEE, INTERNATIONAL INTELLECTUAL PROPERTY: PROBLEMS, CASES, AND MATERIALS 784 (3d ed. 2017) (consumers will knowingly purchase fake luxury goods).

good will associated with the brand name or trademark.[133] In China today (as in many other countries), there is an enormous demand for counterfeit luxury branded handbags that offer the prestige of the genuine brand at a fraction of the price of the genuine product.[134]

The same is true with counterfeit liquor as shown in example (b) above. Consumers in China who purchase counterfeit bottles of famous brand name liquor are not in general buying the liquor for private or personal consumption.[135] In China, for personal or professional reasons, people often have banquets or dinners where highly alcoholic drinks are served and consumed in large quantities as part of social drinking rituals.[136] It is a mark of prestige for a host to serve a famous foreign brand of liquor, such as a French made cognac like Hennessy or a western brand of whiskey such as Johnny Walker Black Label.[137] There is a huge demand for this type of counterfeit liquor, where the counterfeiter uses a bottle that is either a copy or a genuine used bottle and fills it with a cheap but potent liquor.[138] The host can enjoy the good will of serving his guests a high prestige brand while only paying for a common liquor that, while inexpensive, is just as potent but is not contaminated or harmful to the guests.

In the case of (c), young adults in China are highly fashion-conscious and are hungry for famous international brands.[139] Most consumers viewing the webpage with Abercrombie and Fitch pants selling for $12 are fully aware that these are counterfeits and that the product is of low quality. They reason, however, that they can pay about the same price for a low-quality product without the prestige of the counterfeit Abercrombie label or pay a little bit more for the same low-quality product but enjoy the prestige of the Abercrombie brand name. Many consumers will choose the latter.[140]

---

[133] *Id.*

[134] *Id.*

[135] These observations about the use of alcohol in China are based upon the author's own experience and based on discussions with colleagues and associates.

[136] See Nathan H. Gray, *"Gan Bei": Business and Ritualistic Drinking in China*, WORD PRESS (Apr. 22, 2010), https://nathanhgray.wordpress.com/2010/04/22/gam-bei-business-and-ritualistic-drinking-in-china/ (discussing the importance of drinking rituals).

[137] *See* Jiani Ma, *Rich Post-80s Drive Chinese Whiskey Market Growth*, JING DAILY (Apr. 16, 2018), https://jingdaily.com/chinese-whiskey-market/ (noting the demand for premium and super premium brands of whiskey and cognac in China).

[138] Natalie Wang, *Nearly 40% of Chinese Consumers Admit to Purchasing Fake Booze*, THE DRINKS BUS. (Mar. 19, 2018), https://www.thedrinksbusiness.com/2018/03/nearly-40-chinese-consumers-admit-to-purchasing-fake-booze/ (noting that consumers admit to intentionally purchase fake booze in China).

[139] *See e.g.*, *Luxury Brands Tailor Their Marketing to Asian Millennial Consumers*, THE FASHION LAW (Aug. 7, 2018), http://www.thefashionlaw.com/home/luxury-brands-tailor-their-marketing-to-millennial-consumers-in-the-far-east.

[140] This observation is based upon the authors' experience in investigating counterfeit consumer products in China.

2. Alibaba's "Arrogance" and Illegal Activities

While MNCs have consistently complained about Alibaba's tacit approval and support of counterfeiting, these sentiments were recently confirmed for the first time by enforcement authorities in China in connection with an extraordinary national level investigation of Alibaba. The State Administration of Industry and Commerce (SAIC) and its local branches (AICs) are charged with maintaining orderly markets in the PRC and are primarily responsible for stemming the flow of counterfeit goods.[141] In the case of Alibaba, the SAIC took the unprecedented step of conducting an administrative guidance meeting with Alibaba officials in July 2014.[142] The Director of the SAIC emphasized the unique nature of the meeting when he stated, "For this meeting, I didn't know whether it's the first ever of its kind, or the last, but I hope that this would be the last time for a meeting of this nature."[143]

Enforcement actions are usually the provenance of local AICs as the SAIC, the central level authority, is a supervisory and policy-making body.[144] However, the SAIC believed that in the case of Alibaba, it was necessary for the agency to step in to resolve a case that had proven to be intractable to local authorities.[145] In the administrative guidance meeting, the SAIC and appropriate local level AICs met with Alibaba officials in order to set forth an agreed upon set of steps to remediate counterfeiting on Alibaba platforms.[146]

The administrative guidance meeting between the SAIC and Alibaba executives occurred on July 16, 2014,[147] and on January 28, 2015, the SAIC issued a White Paper as a follow up to the meeting to formally set forth a

---

[141] *State Administration of Industry and Commerce*, IP CHANNEL (Feb. 9, 2010), http://ip.people.com.cn/ GB/152255/10960401.html.

[142] *See* Transcript of Administrative Guidance Meeting Between SAIC and Alibaba (held July 14, 2016) (on file with author) [hereinafter Transcript of Admin. Guidance Meeting]; Huang, *supra* note 31 ("On July 16, 2014, the administrative guidance group of the Internet Supervision Department . . . held an administrative guidance forum at the Zhejiang Province Industry and Commerce Bureau. Principal officers and management teams of the core departments of Alibaba Group attended the meeting and accepted administrative guidance."). *See also* Heather Timmons, *Chinese Regulators Flagged Illegal Practices at Alibaba Months Before Its Monster IPO*, QUARTZ (Jan. 28, 2015), https://qz.com/334863/chinese-regulators-flagged-illegal-practices-at-alibaba-months-before-its-monster-ipo/. Administrative guidance is governed by the SAIC's Comprehensive Promotion of Administrative Guidance Work (2009).

[143] Transcript of Admin. Guidance Meeting, *supra* note 142, at 128.

[144] *State Administration of Industry and Commerce*, *supra* note 141 ("The [SAIC] . . . is the competent authority of ministerial level directly under the State Council in charge of market supervision/regulation and related law enforcement through administrative means.").

[145] *See* SAIC WHITE PAPER, *supra* note 31, at 11–12.

[146] The steps were later summarized in the SAIC White Paper. *Id.* at 19.

[147] *See id.*; Huang, *supra* note 31.

plan of remediation.[148] In both the transcript of the meeting and in the SAIC White Paper, the SAIC makes the point repeatedly that at the time of the meeting in July 2014 there were numerous counterfeits, infringing products, and other violations of Chinese laws on advertising, product information, and licensing on Alibaba's websites.[149]

However, the point being made by the SAIC White Paper and during the administrative guidance meeting is more subtle, and even more deep-seated, than the need to control persistent illegal activities. For example, the SAIC states:

> Alibaba Group, for a long time, *has failed to take seriously* the operational violations on its e-commerce platforms and did not take effective measures to address the violations. This caused a miniscule issue to snowball into a serious problem, leading Alibaba to its greatest crisis since its incorporation.[150]

This critique is not directed at practices involving IP rights; it is directed at an underlying culture at Alibaba, which is one of viewing itself as above the law, including an attitude of a willful refusal to obey the law. At another point, the SAIC White Paper states:

> It is suspected that [Alibaba] knowingly, intentionally, by negligence or in spite of their presumed knowledge facilitates unlicensed operations, trademark infringements, untruthful publicity, pyramid schemes and violations of consumers' rights.[151]

The SAIC traces Alibaba's flouting of the law to an attitude of "arrogance."[152] An AIC official at the July 16, 2014 meeting stated that when speaking to Alibaba employees, he felt "a kind of arrogant emotion sprouting and growing."[153] In its White Paper, the SAIC specifically tells Alibaba that it should "redress arrogance."[154] The SAIC informs Alibaba that it cannot expect to "receive special treatment under law. . . . Regulators . . . shall treat businesses equally under law."[155] The SAIC also admonishes Alibaba to "ethically conduct business" and warns that "[a]n enterprise shall not get

[148] *See* SAIC WHITE PAPER, *supra* note 31. The purpose of the White Paper is to provide "various understandings and information about the said administrative guidance meeting" to Alibaba. *See id.* at 11.

[149] Transcript of Admin. Guidance Meeting, *supra* note 142, at 3–8.

[150] SAIC WHITE PAPER, *supra* note 31, at 11–12 (emphasis added).

[151] *Id.* at 14.

[152] *Id.* at 20.

[153] Transcript of Admin. Guidance Meeting, *supra* note 141, at 117.

[154] SAIC WHITE PAPER, *supra* note 31, at 20.

[155] "No market player shall receive special treatment under law. The management of Alibaba family shall understand their bottom line. Regulators in the applicable jurisdiction shall treat businesses equally under law." *Id.*

what it wants at its own will."[156] The SAIC additionally warns Alibaba that it cannot flout the law when it finds the law interferes with its interests and then assert the law when it needs the law's protection despite acting without credibility or integrity.[157]

Although the SAIC stood in the position of a government regulator at the meeting, it at times seemed to descend into the role of a sycophant flattering the Alibaba executives for the purpose of cajoling and pleading with them to respect the law. For example, at the administrative guidance meeting, AIC officials lavishly praised Alibaba, telling the executives how proud the PRC was of their accomplishment,[158] mentioning that all of the Alibaba executives at the meeting were "famous people"[159]and "big shots,"[160] and joking that the monthly salary of just one of the Alibaba executives were as much as the combined annual salaries of all the AIC officials present at the meeting.[161]

a. Specific Practices

Alibaba's lack of respect for the law manifested in two practices that drew the SAIC's special attention and were the focus of discussion during the administrative guidance meeting: taking bribery from the platform participants and colluding with the counterfeiters. The SAIC states that "a large number of Alibaba staffers take business bribes in exchange for giving platform participants [preferential business opportunities] to squeeze out their competitors."[162] While Alibaba was already aware of the bribery problem and took some steps to control it, the AICs stated that bribery was still a problem as of the July 16, 2014 administrative guidance meeting,[163] and an Alibaba vice president at the meeting acknowledged that "temptation from the outside" is a problem among the Alibaba staff.[164] The SAIC also cited Alibaba employees' active participation in misleading consumers and committing various consumer protection violations. For example, the SAIC

[156] *Id.*

[157] "An enterprise shall not get what it wants at its own will, i.e. when needing credibility to protect an enterprise's interest, it boasts about credibility but throws the law away; when needing law to protect itself, it raises up high the flag of law but intentionally ignores its duties regarding credibility and integrity." *Id.*

[158] Transcript of Admin. Guidance Meeting, *supra* note 141, at 13.

[159] *Id.* at 39.

[160] *Id.*

[161] *Id.* at 109.

[162] SAIC WHITE PAPER, *supra* note 31, at 16.

[163] Transcript of Admin. Guidance Meeting, *supra* note 141, at 9 ("The sixth problem is what was included in governance, that is, the commercial bribery existing among the staff of Taobao.com. Suppliers and users of the platform are all involved. You have realized this problem and tried to keep it under control. However, the situation still exists.").

[164] Alibaba executive Xiaofeng Shao: "Recently, we have continued to improve the punishment system, even including the standards for our internal staff because this is also a big problem we face like the temptation from the outside." *Id.* at 92.

notes that "[s]ome of the online shops, through the trading with others, delete negative comments, providing business information to themselves and others that disrupts normal business order . . . . But [Alibaba's] supervision and punishment are not strict enough. There are staff in [Alibaba] involved in this violation."[165] A second set of practices involves Alibaba employees working together with counterfeiters, tipping the counterfeiters off to enforcement actions. For example, an SAIC official stated that in one instance the SAIC asked Alibaba for information about ten online stores suspected of selling counterfeits; although Alibaba provided the information, seven of the stores promptly closed, two cancelled their accounts, and one started to sell authentic products.[166] The SAIC concluded that "[t]his indicated information disclosure by your company staff"[167] to the counterfeiters. In another instance, the SAIC stated that after local AICs provided Taobao, an e-commerce platform owned by Alibaba, with information about their investigations, Taobao was suspected of tipping off counterfeiters and manufacturers of illegal narcotics.[168]

The unlawful activities by Alibaba employees discussed at the administrative guidance meeting in July 2014 came just three years after a major scandal in 2011 that involved about 100 Alibaba employees, including supervisors and sales managers, who after an internal investigation were found to be directly responsible for allowing over 2,300 China Gold Suppliers to defraud international buyers.[169] Long time CEO David Wei Zhe and COO Elvis Lee Shi Huei were forced to resign as a result of the scandal.[170] According to news reports, Alibaba lost $933 million in market share due to the scandal.[171] Three years after this scandal, according to the SAIC, numerous members of Alibaba's staff continued to conduct illegal activities adding further to its perception of a culture of lawlessness at Alibaba.

---

[165] *Id.* at 10.

[166] *Id.* at 11.

[167] *Id.*

[168] SAIC WHITE PAPER, *supra* note 31, at 17.

[169] Pascal-Emmanuel Gobry, *Huge Fraud at China E-Commerce Giant Alibaba.com: Management Out, 100+ Employees Dismissed*, BUS. INSIDER (Feb. 21, 2011), https://www.businessinsider.com/alibaba-ceo-resigns-over-huge-fraud-scandal-2011-2; Kelvin Soh, *Alibaba.com CEO Resigns After Jump in Fraudulent Sales*, REUTERS (Feb. 21, 2011), https://www.reuters.com/article/us-alibaba/alibaba-com-ceo-resigns-after-jump-in-fraudulent-sales-idUSTRE71K1QA20110221 ("'Members of our company's senior management knew of a noticeable increase of fraud claims by global players against China Gold Supplier customers on the international marketplace that began in late 2009,' Ma said in the statement.").

[170] Gobry, *supra* note 169; Soh, *supra* note 169.

[171] Mark Lee, *Alibaba Shares Tumble After Fraud Leads to CEO Departure*, BLOOMBERG (Feb. 22, 2011), https://www.bloomberg.com/news/articles/2011-02-22/alibaba-comdown graded-by-morgan-stanley-after-ceo-wei-resigns.

b. Above the Law in China

Alibaba's "arrogance" needs to be understood in the context of China's legal and political culture. In China today, it is not unusual for powerful entities to routinely disregard the law. In general, the more powerful an entity, the less compelled it feels to follow the law. Alibaba is among a handful of the most powerful entities in China. As a mundane example familiar to every citizen in China, cars registered to the People's Liberation Army ("PLA") do not obey traffic laws.[172] Every car registered to the PLA has a special license plate. These cars will routinely drive through red lights, speed, and refuse to pay tolls. Under China's current security systems, cars that drive through red lights are recorded by cameras stationed at every traffic stop, and letters containing fines are sent to transgressors. PLA cars, however, do not pay fines. No regular police officer with the Public Security Bureau will dare to stop a PLA car for a traffic violation, and no toll collector will dare to challenge a PLA car that refuses to pay the toll. This is a deeply embedded cultural attitude that starts at the top with the most powerful entity of all in Chinese society: the Communist Party, which views itself as above the law and views the law as a mere instrument for it to use to achieve its own ends.[173] These Party attitudes will be familiar to Jack Ma, the chairman of Alibaba, who is also a member of the Communist Party,[174] as are other senior Alibaba executives.[175]

As noted earlier, Alibaba's size is prodigious, and its financial power overwhelming.[176] In China today, an entity that is as large and powerful as Alibaba does not believe that it needs to answer to lowly government enforcement officials. Alibaba executives, such as Chairman Jack Ma, himself a Communist Party member, and other senior Alibaba officials who are also Party members, believe that they do not answer to the law but only to the Party, the ultimate authority in China.[177] One example of the close link between Alibaba and the Party is that Alibaba runs China's new social credit system.[178] Alibaba assigns a three digit score (from 350 to 950) to each citizen in China based on the social desirability of the citizen's conduct,

[172] The author has witnessed these practices by the PLA firsthand in China.

[173] DANIEL C.K. CHOW, THE LEGAL SYSTEM OF CHINA IN A NUTSHELL 62 (3d ed. 2015): "[N]either Imperial China nor pre-reform modern China recognized or accept the rule of law . . . . [T]he Communist Party views itself as holding unchallenged authority. In modern China, the Communist Party is supreme."

[174] Li Yuan, *Jack Ma, China's Richest Man Belongs to the Communist Party. Of Course.*, N.Y. TIMES (Nov. 27, 2018), https://www.nytimes.com/2018/11/27/business/jack-ma-communist-party-alibaba.html.

[175] The author has personal knowledge that senior Alibaba officials are Party members from his current work as a legal expert in litigation involving China.

[176] *See supra* text accompanying notes 103–107.

[177] This observation is based upon the author's own assessment and analysis.

[178] Campbell, *supra* note 42.

allowing the government to punish or reward its citizens.[179] These close ties further suggest that Alibaba is not intimidated by and does not fear PRC enforcement authorities. For their part, PRC enforcement authorities are reluctant to shut down or seriously harm Alibaba because such actions will lead to significant financial losses for China and the possible demise of one of the world's leading technology companies and a great source of national pride.[180]

An indication of how Alibaba continues to view itself as above the law in China is that on April 25, 2019, the USTR placed Alibaba on its Notorious Markets List for the third year in a row.[181] This designation occurred five years after the SAIC administrative guidance meeting in July 2014 and four years after the SAIC issued the White Paper detailing a plan of remediation in 2015. In its 2018 report, the USTR stated, "[a]lthough Alibaba has taken some steps to curb the offer and sale of infringing products, right holders . . . continue to report high volumes of infringing products and problems with using takedown procedures."[182] After a history of misconduct, scandals, vehement protests by brand owners, an extraordinary effort by the PRC government, and numerous blacklists by the U.S. government, Alibaba's conduct has not changed appreciably. Under these circumstances, brand owners must confront the reality that Alibaba is not likely to change its conduct without intervention by the highest levels of the Party, probably only by a personal decision by Xi Jinping, China's President and the General Secretary of the Communist Party.[183] Until senior Party leaders intervene, brand owners must accept the likelihood that Alibaba believes that it can operate outside of the law in China with impunity and without fear of government reprisals.

E. Amazon

Amazon is currently the largest e-commerce marketplace in the United States[184] and is the second largest in the world, trailing only Alibaba.[185] As of 2016, the market value of Amazon exceeded that of the eight largest U.S. brick-and-mortar retailers combined, including Walmart, Target, and Best

---

[179] *Id.*

[180] This observation is based upon the author's assessment of the overall tone of the SAIC White Paper, *supra* note 31, and the transcript of the administration guidance meeting, *supra* note 141.

[181] OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, SUPRA NOTE 114.

[182] *Id.*

[183] This is the author's professional opinion based on his experience and knowledge of China. For a summary of Xi's positions, *see President Xi Jinping*, THE U.S.-CHINA BUS. COUNCIL, https://www.uschina.org/president-xi-jinping (last visited July 1, 2019). *See also #1 Xi Jinping*, FORBES, https://www.forbes.com/profile/xi-jinping/#2f2f40051601 (last visited July 1, 2019) (President Xi became the "core" leader of the Communist Party in 2016.).

[184] *See* Levy, *supra* note 107.

[185] *See id.*

Buy.[186] In December 2018, Amazon's GMV reached $239 billion.[187] One of its most popular online retail services, Amazon Prime, now has over 100 million members worldwide.[188] Amazon's official anti-counterfeiting policy states that it is the responsibility of the seller or supplier to ensure that its products are genuine, not counterfeits.[189] Two aspects of Amazon's business practices have led to a rise in online counterfeits.

Once a brand owner agrees to sell its products on Amazon's e-commerce marketplace, Amazon will source products not only from the brand owner, but also from other third-party vendors that sell the branded products. In order to have sufficient inventory on hand to satisfy customer orders expeditiously, Amazon's warehouses will co-mingle products from the brand owner and from other third-party vendors into a single source of supply.[190] If a third-party vendor ships a counterfeit product to Amazon, it becomes co-mingled with genuine products in Amazon's warehouse. When a customer orders a product online, the customer may receive a product from the warehouse from either the brand owner or a third-party vendor, which might be a counterfeit. The source of the product is not clear to the customer when he or she makes a purchase, but the customer will generally assume that it was manufactured by the brand owner.

Unable to make inroads into China's e-commerce marketplace against competitors such as Alibaba, Amazon decided in 2015 to woo Chinese manufacturers to sell directly to U.S. consumers on its e-commerce site.[191] As China is the world's largest source of counterfeits, the result was predictable: beginning in 2015, counterfeits soon began to proliferate on Amazon's e-commerce sites, much to the chagrin and exasperation of brand owners. Brand owners' complaints against Amazon also echo some of the complaints against Alibaba. For example, according to one brand owner representative, "Amazon is making money hand over fist from counterfeiters, and they've done about as little as possible for as long as possible to address the issue."[192]

---

[186] Jeff Desjardins, *The Extraordinary Size of Amazon in One Chart*, VISUAL CAPITALIST (Dec. 30, 2016), https://www.visualcapitalist.com/extraordinary-size-amazon-one-chart/.

[187] *See* Levy, *supra* note 107.

[188] Austen Hufford & Georgia Wells, *Amazon Prime Has More Than 100 Million Members*, WALL ST. J. (Apr. 18, 2018), https://www.wsj.com/articles/amazon-prime-has-more-than-100-million-members-1524088630.

[189] *Amazon Anti-Counterfeiting Policy*, AMAZON, https://sellercentral.amazon.com/gp/help/external/201165970 (last visited July 1, 2019).

[190] Pierson, *supra* note 13.

[191] Shepard, *supra* note 9.

[192] Levy, *supra* note 18.

III. ENTITY VERIFICATION MEASURES AND THE REQUIREMENTS OF PRC LAW

The discussion in Part II centers on how the concern is different in each case, although brand owners voice similar concerns about counterfeits available on Alibaba and Amazon. The major complaint by brand owners with Alibaba is that it facilitates the sale of counterfeits in order to satiate the enormous appetite for counterfeits among China's consumers. In the case of Amazon, the major concern of brand owners is that U.S. consumers who seek to purchase genuine products are instead deceived into purchasing a counterfeit. In both cases, brand owners have expressed frustration with the lack of effective enforcement by these e-commerce platforms against webpages or postings selling counterfeits on Alibaba or Amazon's websites. These problems are further discussed below.

A. Problems with Enforcement

Although brand owners have many complaints about enforcement issues against counterfeiters on Alibaba and Amazon platforms, the crux of these complaints can be summarized as follows: (1) counterfeiters use false identities and addresses and thus are untraceable; (2) brand owners must suffer through the use of cumbersome and ineffective notice and takedown procedures; and (3) existing measures used by e-commerce platforms do not deter repeat infringing activity.

1. False Names, Identities, and Addresses

Current e-commerce platforms, including Alibaba and Amazon, do not subject new sellers to adequate verification or confirmation although Alibaba is required to do so under PRC law; without an enforced verification or confirmation process, counterfeiters routinely use false or inaccurate names and addresses when registering with these e-commerce platforms.[193] When brand owners pursue counterfeiters in enforcement actions, they discover that names and addresses are fictional, and the counterfeiters then disappear into the vast expanse of cyberspace. Brand owners argue that Alibaba and Amazon have few requirements for registration and that verification of this information is not thorough or adequate. In the case of Alibaba, the SAIC White Paper stated that "only lip service is paid to credential review and registration of vendors."[194] Brand owners often complain that vendors on Amazon use fictitious names and addresses.[195]

2. Burdensome Notice and Takedown Procedures

E-commerce platforms create bureaucratic or technical hurdles in

[193] SAIC WHITE PAPER, *supra* note 31, at 13.

[194] *Id.*

[195] *See* [a hereinafter reference], *supra* note 13.

helping brand owners to locate or identify sources of counterfeits and counterfeiters.[196] These hurdles delay, frustrate, and create additional financial burdens for brand owners.[197] Both Amazon and Alibaba use a notice and takedown procedure that is based upon requirements set forth in the DMCA[198] and similar provisions in PRC law, respectively.[199] When a brand owner discovers an offending webpage or posting, the brand owner is required to submit notices to the ISP under a certain set of criteria that results in the ISP requiring the removal of an offending webpage or posting. Brand owners have described the experience of using notice and takedown procedures as "Kafka-esque"[200] and likened their use to being imprisoned in "Amazon purgatory."[201] Brand owners are required to place an order for the counterfeit goods, buy and receive the goods from the offending website, test the goods, verify that they are counterfeit, and then submit both the counterfeit and genuine product with notices documenting these actions.[202] Alibaba has a "three strikes" policy,[203] requiring proof of three completed transactions involving counterfeits and submission of notices before an offending webpage can be removed. This process can take months, is expensive, and consumes significant time and effort by the brand owner. Even when brand owners satisfy this arduous process, they complain that the notices are still often ultimately rejected for technical reasons.[204]

3. Lack of Deterrence

In those instances in which brand owners can achieve a takedown of the offending website or otherwise bring pressure to bear on counterfeiters, brand owners complain that once the counterfeit goods disappear, they reappear in short order on a new webpage.[205] Some brand owners refer to this process as a futile game of "Whac-A-Mole" in which a counterfeiter disappears only to immediately reemerge under a new name, identity, and location to resume its counterfeiting operations.[206] In the meanwhile, brand owners have expended significant time, effort, and money in pursuing the

---

[196] *See supra* text accompanying note 15; *see also supra* text accompanying note 101.

[197] *See* Bercovici, *supra* note 15.

[198] *See* 17 U.S.C. § 512 (Westlaw through Pub. L. No. 116-68). *See also Intellectual Property Policy for Sellers*, *supra* note 101 (Amazon); *Intellectual Property Rights (IPR) Protection Policy*, *supra* note 101 (Alibaba).

[199] *See generally* Trademark Law of the People's Republic of China, *supra* note 97; Law Against Unfair Competition of the People's Republic of China, *supra* note 97.

[200] Bercovici, *supra* note 15.

[201] *Id.*

[202] *Id.*

[203] *Enforcement Actions for Intellectual Property Rights Infringements Claims on Alibaba.com*, ALIBABA (Nov. 1, 2017), https://rule.alibaba.com/rule/detail/2043.htm.

[204] *See* Bercovici, *supra* note 15.

[205] *See supra* text accompanying note 15.

[206] Bercovici, *supra* note 15.

counterfeiting without achieving any tangible results.

B. Proposed Remedial Measures

While counterfeiting on the Internet is a daunting problem, China provides the information technology tools that can be used to deter counterfeiters and that can address each of the three major enforcement issues faced by brand owners: false identities and addresses, convoluted notice and takedown procedures, and rampant recidivism. Most brand owners are completely unaware of or otherwise do not understand these potent tools.

1. AIC Business License

As part of China's extensive system of industrial and social control, a legal regime of identification and attribution of legal liability exists that can be used against counterfeiters involved in e-commerce commerce. Both in the July 16, 2014 administrative guidance meeting and in its White Paper, the SAIC repeatedly refers to Alibaba's need to control counterfeiting at the point of entry (i.e., registration on the Alibaba websites). The AICs stressed that if entry is well controlled, many of Alibaba's current problems can be solved.[207] This Article argues that brand owners should heed the advice of China's enforcement authorities and seek to have e-commerce platforms implement effective registration procedures in accordance with the specific requirements of PRC law. These measures can create prophylactic measures at the point of entry that can create an effective deterrent to counterfeiting.

Article 23 of SAIC Order No. 60, Measures on the Administration of Online Transactions ("MAOT")[208] requires business operators of online platforms to verify the legal identities of all entities or persons applying for access to their platform for the sale of products:

> The business operator of a third-party transaction platform shall examine and register as business operators the identities of the legal persons, other economic organizations or industrial and commercial sole proprietors that apply for access to the said platform for sale of products or provision of services, establish registration files and conduct regular verification and updating, and *make public the information specified in their business licenses or provide electronic links to their business licenses in eye-catching locations on its main web pages for business activities*.[209]

As set forth above, Article 23 requires the e-commerce platform to display information in the business licenses of business operators or to

[207] Hua Yu of Fujian Provincial AIC: "Until now, it seems that there are some difficulties in solving some problems. But in fact, if the entity is well controlled, I don't think it will be a problem." Transcript of Admin. Guidance Meeting, *supra* note 141, at 27.

[208] *See* Administrative Measures for Online Trading, *supra* note 48.

[209] *Id.* at art. 23 (emphasis added).

provide a link to their business licenses.[210] Under PRC law, every lawful business entity in the PRC must have a business license issued by the local AICs that contains the lawful business scope of the entity, its address, and the name of its legal representative.[211] All lawful enterprises must have an official, AIC-issued business license; any entity that does not have a business license cannot lawfully operate.[212]Business operators obtain a business license by applying to local AICs that review their proposed business operations to ascertain that they are lawful and economically feasible.[213] For example, if a business operator proposes to sell trademarked products, the AICs will ask for proof of a trademark registration or trademark licensing agreement.[214] The issuance of a business license means that the AICs have reviewed and approved the proposed business plan of the applicant and found it to be lawful.

Among its other functions, the business license sets forth the lawful business scope of the entity. For example, a business license might state that the entity is lawfully authorized to engage in the sale of laundry detergent or other cleansing agents for laundry. Such an entity would be acting unlawfully if it engaged in any business outside of that scope, such as, for example, the sale of peripheral equipment for computers or mobile phones. A business operator that obtains a business license for the sale of genuine products but instead sells counterfeits is in violation of its license and faces a fine or suspension of the license, which would require ceasing business operations.

The business license also prevents the business operator from using a business name and address on an e-commerce site different from that on the business license. Only the business identified in the license by its name and address is lawfully entitled to use the business license, i.e. such licenses are not transferable and cannot be used by an entity other than the one that

---

[210] *Id.*

[211] Companies Law of the People's Republic of China, ch. I, art. 7 (promulgated by the President of the PRC, Order No. 42, Oct. 27, 2005, effective on Jan. 1, 2006) ("The business license for a company shall state therein such matters as the name, domicile, registered capital, actual paid-up capital, business scope, the name of the legal representative, etc.") [hereinafter Companies Law of the PRC].

[212] *See id.* ("Company registration authorities shall issue business licenses for companies established under the law. The date of issuance of a business license for a company shall be the date of establishment of the company."). *See National Enterprise Credit Information Publicity System*, SAIC, http://www.gsxt.gov.cn/index.html (last visited July 1, 2019). *See also The 5-in-1 China Business License (WFOE/WOFE)*, FDI CHINA (July 11, 2018), https://www.fdichina.com/blog/china-company-registration/wfoe-wofe/5-in-1-business-license/.

[213] This observation is based upon the author's own experience in applying for business licenses in China. *See* Matt Slater, *What Is a China AIC?*, CHINA CHECKUP (Dec. 9, 2013), https://www.chinacheckup.com/blogs/articles/china-aic ("China AICs . . . provide official registration records for all companies in their jurisdiction[.]").

[214] The author has applied for business licenses in China and was asked by the AIC to provide proof of ownership or authorized use of trademark rights for products sold under the mark to ensure that the business had the legal right to sell the branded products.

applied for and received the business license. A business operator that has sold counterfeit goods and that has been the subject of an enforcement action cannot just simply disappear and reappear on the Internet under a different business name and address; if the name and address do not match that on the license, the use of the license is unlawful. Strictly verifying the information on the business license will prevent business operators accused of counterfeiting from disappearing and immediately reappearing under a different name and address. To use a different name and address, the business operator would have to apply for a new business license from the AIC, a process that could take months.[215]

Requiring a valid business license will preclude many underground counterfeiting factories, petty criminal organizations, smugglers, and other illegal entities from registering to sell on an e-commerce platform because such entities are unwilling to undergo scrutiny by the AICs for fear that their illegal activities will be exposed, leading to prosecution by AICs and other PRC authorities, such as the Public Security Bureau (the police). These types of nefarious entities and persons are also involved in brick-and-mortar counterfeiting; they operate illegal underground factories and have no business licenses.[216] However, without a valid business license, these entities will be unable to register on an e-commerce platform such as Alibaba in accordance with Article 23 of the MAOT.

2. Legal Representative

The business license will also contain the name of the business entity's legal representative.[217] Under PRC law, every lawful business must have a natural person who serves as the legal representative of the business entity.[218] According to PRC law, the legal representative has the clear authority to act on behalf of the business entity and can bind the business entity to contracts and other legal relationships.[219] In many cases, the chairman of the board of directors of a company or a person of a similar rank in other organizations will serve as the legal representative.[220] PRC authorities wanted to make sure that under the law, it was always clear which person within a business enterprise could sign a legally binding contract or create other legal

[215] This observation is based on the author's own personal experience in applying for business licenses in China.

[216] The author's own experience is that many of these counterfeiters do not operate their businesses within the boundaries of the laws and regulations.

[217] Companies Law of the PRC, *supra* note 211, at ch. I, art. 7

[218] General Principles of the Civil Law of the PRC, *supra* note 51, at ch. III, art. 38 ("In accordance with the law or the articles of association of the legal person, the responsible person who acts on behalf of the legal person in exercising its functions and powers shall be its legal representative.").

[219] *Id.*

[220] Any person can serve as a legal representative, but companies usually appoint a high ranking official.

relationships.[221] Although not specifically required by the MAOT, e-commerce platforms should require the business entity's legal representative to undergo the registration procedures so as to make certain that the business entity has lawfully committed to legal obligations created by registration.

Under PRC law, the legal representative is also personally subject to administrative and criminal liability whenever the company conducts illegal operations beyond the range approved by registration authorities, commits fraud, secretly withdraws or transfers funds, or engages in other illegal activities.[222] The existence of the legal representative ensures the PRC government that there is always a flesh and blood person who will be responsible to PRC authorities for violations of the law by legal "persons," such as a business enterprise. [223] PRC authorities did not want ultimate civil or criminal liability to rest solely with a legal fiction while natural persons escaped responsibility.[224]

By identifying a business entity's legal representative through requiring submission of its business license, e-commerce platforms such as Alibaba would provide the brand owner with a flesh and blood person against whom it can directly bring a complaint in a civil lawsuit under the PRC Trademark Law[225] or Anti-Unfair Competition Law[226] or whom the Public Security Bureau (the police) can arrest under the PRC Criminal Law.[227]

With these requirements, brand owners would not be limited to using the e-commerce platform owner's internal enforcement mechanism, such as

---

[221] General Principles of the Civil Law of the PRC, *supra* note 51, at ch. III, art. 38.

[222] General Principles of Civil Law of the People's Republic of China, Article 49:

Under any of the following circumstances, an enterprise as legal person shall bear liability, its legal representative may additionally be given administrative sanctions and fined and, if the offence constitutes a crime, criminal responsibility shall be investigated in accordance with the law:

(1) conducting illegal operations beyond the range approved and registered by the registration authority;

(2) concealing facts from the registration and tax authorities and practicing fraud;

(3) secretly withdrawing funds or hiding property to evade repayment of debts;

(4) disposing of property without authorization after the enterprise is dissolved, disbanded or declared bankrupt;

(5) failing to apply for registration and make a public announcement promptly when the enterprise undergoes a change or terminates, thus causing interested persons to suffer heavy losses;

(6) engaging in other activities prohibited by law, damaging the interests of the State or the public interest.

General Principles of the Civil Law of the PRC, *supra* note 51, at ch. II, art. 49.

[223] General Principles of the Civil Law of the PRC, *supra* note 51, at ch. III, arts. 38 & 49.

[224] *Id.*

[225] Trademark Law of the People's Republic of China, *supra* note 97.

[226] Law Against Unfair Competition of the People's Republic of China, *supra* note 97.

[227] Selling counterfeits violates Article 140 of the Criminal Law of the People's Republic of China. *See* Criminal Law of the People's Republic of China, ch. III, art. 140 (promulgated by the President of the PRC, Order No. 83, Mar. 14, 1997).

the notice and takedown procedures. As PRC law requires that the business operator make its business license available on the e-commerce platform and as business licenses are publicly available on the AIC websites, the brand owner does not need to go through the platform owner to obtain the necessary information to directly pursue the business operator.[228] Instead, the brand owner can immediately act against the legal representative listed in the business license upon discovering an offending webpage or posting rather than be subject to the long and frustrating delays of the notice and takedown procedures. Of course, the brand owner can also use the platform owner's internal procedures in addition to bringing an action directly against the business operator through PRC enforcement authorities or, under some circumstances, in the United States if the offender has sufficient U.S. contacts.[229]

The use of an enforcement method that does not rely on the active participation of the e-commerce platform is particularly useful in the case of Alibaba, which the PRC authorities themselves have identified as viewing itself above the law. Any method of enforcement against counterfeiters that requires the active participation of Alibaba could be met with half-hearted efforts or resistance, as many brand owners have persistently suspected and complained. Directly pursuing the counterfeiter will also relieve brand owners from the burden of using Amazon's convoluted internal procedures.

3. Verification and Deterrence

Requiring, verifying, and displaying seller information should create an effective deterrent against selling counterfeits on Alibaba and other e-commerce platforms, since fewer counterfeit sellers would even turn to the platform in the first place if such sufficient safeguards were in place. Counterfeiters always rely on the use of false identities, false names, and false addresses because they are fearful of detection, capture, arrest, and prosecution.[230] This is true of counterfeiters who sell in brick-and-mortar outlets as well as counterfeiters who sell on the Internet. The essential tools

[228] A similar procedure can be used in the case of sole proprietorships that would require individuals to register, i.e. Alibaba should do a strict review of the identity card of the registrant. "A natural person who intends to engage in online product transactions shall carry out business activities via a third-party transaction platform, and submit to the third-party transaction platform his/her name, address, valid identity proof, valid contact details and other real identity information." General Principles of the Civil Law of the PRC, *supra* note 51, at ch. I, art. 7. The same principle applies: identifying the name and address of a flesh and blood person who can be held civilly and criminally responsible can be an effective deterrent against counterfeits on Alibaba websites.

[229] It would be possible to file an action against a Chinese counterfeiter in the United States only if the counterfeiter is subject to the personal jurisdiction of U.S. courts under the minimum contacts standard set forth in *Int'l Shoe v. Wash.*, 326 U.S. 310 (1945) and its progeny.

[230] This observation is based on the author's own extensive experience in pursuing counterfeiters in China and in the United States.

of the counterfeiter are secrecy, subterfuge, and artifice. The counterfeiter relies on these tools to disappear at the first sign of trouble. Denying the counterfeiter the use of these tools of secrecy and disguise would force the counterfeiter to operate openly and transparently subject to legal actions in China or in the United States, a prospect that counterfeiters abhor. Many counterfeiters would find the price of transparency and the risks of capture too high a price to pay for operating on the Internet and, as a result, will be deterred from registering on e-commerce platforms.

Currently, however, as the SAIC notes, Alibaba "only pays lip service"[231] to verifying information. The SAIC specifically criticized Alibaba for numerous careless and lax practices in its examination of business licenses that fail to verify that the entity named in the business license was the user of the license.[232] A review of the Alibaba webpages contained in the Appendix indicates the business operator has not displayed or provided access to its business license on its webpage as required by Article 23 of the MAOT.[233] At present, many individuals register on Alibaba's websites by using false identification papers, sets of which—as the SAIC noted—can be purchased on Alibaba's websites.[234] Under its guidelines, Amazon does not require online sellers from China to submit an AIC business license or identify a legal representative. Currently, Amazon only requires a business name, a telephone number, and some form of personal identification, and, as a result, many vendors provide fictitious information.[235]

4. Amazon and PRC Law

Although Alibaba is clearly subject to the SAIC Measures on the Administration of Online Transactions, it is arguable that Amazon is also subject to these provisions as applied to business entities in China that register on Amazon. Under traditional choice of law principles, the physical location of the business entities in China provides a basis for choosing Chinese law to govern the matter of the registration of those entities.[236] Even

---

[231] SAIC WHITE PAPER, *supra* note 31, at 13.

[232] "Some online stores that are required to upload business licenses to pass the true name authentication have an entity name, business address, residential information that apparently are not consistent with the entity name, business address or residential address on the business license. Some vendors uploaded business license information of other companies." *Id.*

[233] *See* Appendices 1-3.

[234] Transcript of Admin. Guidance Meeting, *supra* note 142, at 98.

[235] *Selling on Amazon: Frequently Asked Questions*, *supra* note 44 (requiring a business name, address, and contact information among other information in order to open an Amazon seller account); *see also supra* note 13 (brand owners find vendors provide bogus information).

[236] Under the Restatement (Second) of Conflicts of Law § 188(2), the following factors would support a finding of PRC law to govern the registration requirements: (a) place of contracting, (c) place of performance, (d) location of the subject matter of the contract, and (e) place of incorporation and place of business of the parties. Restatement (Second) of Conflicts of Law § 188(2) (Am. Law Inst. 1971).

if choice of law rules do not dictate the application of the SAIC Measures, nothing prevents Amazon from choosing on its own, through a choice of law clause in its contracts with vendors, to follow PRC law and require each Chinese business to submit an AIC business license or a link to the license on its websites as well as requiring the legal representative to undergo registration procedures.[237] This process will allow brand owners in the United States to bring an action directly against business operators in China that use offending webpages or posts on Amazon in lieu of or in addition to pursing notice and takedown procedures. As the vast majority of counterfeits originate from China,[238] such measures could be an effective deterrent to counterfeits on Amazon.

5. Consent to Arbitration before CIETAC

Although not required by MAOT or other PRC law, e-commerce sites should also include in their registration procedures a clause requiring the resolution of disputes involving foreign elements by arbitration before the China International Economic and Trade Arbitration Commission (CIETAC).[239] CIETAC has its headquarters in Beijing and facilities in other cities in China and Hong Kong;[240] it lists many foreign experts among its roster of arbitrators,[241] and parties can choose English as the language of the arbitration.[242] The clause should include a provision that the business operator consents to the arbitration of disputes with the platform owner or an entity authorized by the platform owner, i.e., the brand owner.

Arbitration clauses providing for resolution of disputes by CIETAC are now commonly used by many companies to resolve international business disputes that involve China,[243] and arbitration is generally the normal method for resolving international disputes.[244] The advantage of such a clause for the brand owner is the certainty that an action can be filed against the legal

---

[237] Parties can also choose the applicable law through a choice of law provision. *See id.* § 187.

[238] *See supra* Part II.A.

[239] China Int'l Econ. & Trade Arbitration Comm'n (CIETAC) Arbitration Rules, art. 3(2) (revised and adopted by the China Council for the Promotion of International Trade and China Chamber of International Commerce on Nov. 4, 2014 and effective on Jan. 1, 2015), http://www.cietac.org/Uploads/201904/5caae5be03bb5.pdf [hereinafter CIETAC Arbitration Rules].

[240] CIETAC Arbitration Rules, *supra* note 239, art. 2(3).

[241] *Arbitrators*, CIETAC, http://www.cietac.org/index.php?g=User&m=Arbitrator&a=index&l=en (last visited July 1, 2019).

[242] CIETAC Arbitration Rules, *supra* note 239, art. 30.

[243] *See Model Clause: China International Economic and Trade Arbitration Commission (CIETAC)*, INT'L TRADE CENTR., http://www.intracen.org/Model-Clause-China-International-Economic-and-Trade-Arbitration-Commission-CIETAC/ (last visited July 1, 2019) (promoting the use of a model arbitration clause using the CIETAC).

[244] CHOW & SCHOENBAUM, *supra* note 55, at 593 (noting that arbitration is now the normal way to resolve international business disputes).

representative of the business operator with CIETAC and that CIETAC will have jurisdiction over the respondent. This will allow brand owners to move expeditiously when filing an action with CIETAC without having to deal with the uncertainty of preliminary issues such as proper notice and jurisdiction in a court-based litigation. The brand owner will also not need to suffer through the agony of waiting months required by using notice and takedown procedures.

CIETAC awards enjoy a high degree of respect and enforceability in China. PRC law requires parties to implement CIETAC arbitral awards[245] and the awards are enforceable by Chinese courts at the local level.[246] Consent to arbitration before a prestigious entity such as CIETAC would act as a further powerful deterrent to counterfeiters in China, who are used to dodging legal authorities not consenting to appear before them. The threat of being brought before CIETAC should further deter counterfeiters from registering on e-commerce platforms. For those merchants that do register, brand owners will have a quick and effective method of enforcement.

IV. CONCLUSION

The dawn of the age of e-commerce in the new millennium opened new possibilities for legitimate commerce, but it also created vast new opportunities for illegal commerce, such as the sales of counterfeits on a previously impossible scale and level of penetration. This Article has detailed some of the daunting challenges the Internet created for brand owners and the brand owners' numerous but frustrated efforts in dealing with this potent new threat.

This study has focused on the two largest e-commerce sites in the world that dominate online retail services in China and the United States and the lessons learned can be immediately applied to other sites. The kinds of problems that brand owners face on Alibaba and Amazon are both different and similar.

The problems are different in that Alibaba facilitates the sale of counterfeits to satiate the enormous demand for counterfeits by Chinese consumers, whereas Amazon sells counterfeits on its e-commerce site to U.S. consumers who are deceived into buying a counterfeit when they sought to buy a genuine product. Together, Alibaba and Amazon can deliver a crippling one-two punch to brand owners: Alibaba facilitates the sale of counterfeits of their products to those consumers who seek them, and Amazon facilitates the sale of counterfeits to those who do not. Considering

[245] CIETAC Arbitration Rules, *supra* note 239, art. 55(1) ("The parties shall perform the arbitral award within the time period specified in the award. If no time period is specified in the award, the parties shall perform the award immediately.")

[246] CIETAC Arbitration Rules, *supra* note 239, art. 55(2) ("Where one party fails to perform the award, the other party may apply to a competent court for enforcement of the award in accordance with the law.")

that there are other huge e-commerce sites such as JD.com and Tencent in China and e-Bay and Groupon in the United States with similar issues, brand owners are faced with numerous dangerous threats.

The problems are similar in that brand owners find the pursuit of counterfeiters through these two e-commerce giants to be frustrating and ineffective and the direct pursuit of counterfeiters to be futile, as counterfeiters quickly vanish into cyberspace at the first sign of trouble.

Both sets of problems can be remediated through the suggested course of action set forth in this Article. However, while brand owners have made many demands to Alibaba and Amazon to streamline and improve their internal procedures for the monitoring of counterfeits and their notice and takedown procedures, to the best of the author's knowledge, no brand owner has looked closely at PRC law for help despite the urging of PRC officials.[247] Given the poor reputation of China in protecting foreign intellectual property rights,[248] this lack of trust in PRC law is understandable, but information technology tools are available that can be put to effective use. Of course, these tools were not created by the PRC with the goal of protecting foreign brand owners, but instead for the purpose of satisfying China's obsessive need to closely monitor all aspects of Chinese civil society. While China is far behind the United States in protecting intellectual property rights, China is far ahead of most countries in using information technology to monitor and supervise all aspects of Chinese civil society.[249] These tools can provide a level of effective deterrence to Chinese counterfeiters that seek to sell their illegal wares on internet commerce sites based in China or the United States. Brand owners can use the tools detailed in this Article on their own, or in conjunction with existing and developing new tools through internet commerce sites as an overall strategy of deterrence.

To be able to use the tools discussed in this Article, brand owners only need to insist on what they have every right to receive: e-commerce sites in China, such as Alibaba, must faithfully obey relevant provisions of PRC law that are simple and straightforward, an area in which Alibaba falls far short;[250] and e-commerce sites in the United States, including Amazon, should apply PRC law on entity registration of Chinese business operators

---

[247] *See supra* note 206.

[248] *See* Daniel C.K. Chow, *The Myth of China's Open Market Reforms and the World Trade Organization*, U. PENN. J. INT'L L. 8 (forthcoming 2019) (file on copy with the author).

[249] One example is China's recent social credit system, which involves assigning a social credit score indicating the desirability of a citizen's conduct to each citizen in China, a country of over 1.38 billion people. *See supra* note 42. There is also a more menacing side to China's use of technology in monitoring its citizens. Critics have argued that China has used advanced technology to create an "all seeing police state" in the rebellious Muslim-dominated area of Xinjiang Province. *See China's Hi-Tech Police State in Fractious Xinjiang a Boon for Security Firms*, S. CHINA MORNING POST (Jun. 27, 2018), https://www.scmp.com/news/china/diplomacy-defence/article/2152749/chinas-hi-tech-police-state-fractious-xinjiang-boon.

[250] *See supra* Part II.D.2.

under traditional choice of law rules, a choice of law clause, or voluntarily. Verification of entity registration should become easier with the enactment of proposed new data security legislation that would impose civil and criminal liability for the misuse of electronic information.[251] Entities that register on e-commerce sites could become liable for the use of false, misleading, or inaccurate business licenses and thus would have an additional legal incentive to use business licenses accurately. [252]

Alibaba poses a particularly formidable challenge to brand owners due to its overwhelming size and power within China and its leading role in facilitating the online sale of counterfeits. Alibaba's prodigious wealth and strength has led, in the words of PRC officials, to a culture of "arrogance."[253] Brand owners have suspected for years that Alibaba tacitly tolerates and supports counterfeiting in order to earn revenue from these sales. Recently, PRC national government authorities have confirmed these suspicions as the result of an extraordinary national-level intervention intended to discipline Alibaba. Beyond tolerating and supporting counterfeiting, Alibaba, in the words of PRC national authorities, views itself as above the law and unafraid of and not intimidated by PRC enforcement authorities.[254] In fact, the opposite seems to be the case, as the 2014 investigation of Alibaba by the SAIC indicates: government authorities are reluctant to seriously discipline Alibaba or its business due to Alibaba's exalted stature and reputation as a national paragon in China.[255] This raises a deeper issue with Alibaba for brand owners, as this attitude is unlikely to change without intervention by the highest levels of the Communist Party, a topic that deserves further scholarly exploration but is beyond the scope of this Article.

The proposed course of action described in this Article has the advantage of not having to rely on Alibaba's active participation; all that is required is that Alibaba mechanically apply the law as is required for registration of online vendors, and brand owners can on their own enforce their rights against offending parties in civil and criminal actions in China or the United States. The proposals set forth in this Article also apply to problems that brand owners face on Amazon and other U.S.-based e-commerce sites, so long as these sites apply PRC law as a result of choice of law analysis, a choice of law clause, or voluntarily. So long as Amazon follows PRC law in entity registration verification, brand owners can proceed directly with legal actions against counterfeiters and infringers in China or

---

[251] Shuju Anquan Guanli Banfa (Zhengjiu Yijian Gao) Di Si Tiao (数据安全管理办法（征求意见稿）第四条), *translated in* Security Measures for Data Security Management (Draft for Comments), art. 4, COVINGTON UNOFFICIAL TRANSLATION, https://www.inside privacy.com/wp-content/uploads/sites/6/2019/05/Measures-for-Data-Security-Management_Bilingual-1.pdf (last visited Nov. 25, 2019).

[252] *Id.*

[253] *See supra* text accompanying note 151.

[254] *See supra* text accompanying notes 151-156.

[255] *See supra* text accompanying note 182.

the United States and are not relegated to the misery of relying solely on Amazon's convoluted and cumbersome internal procedures.

Ironically, while most brand owners have focused their attention on streamlining the internal monitoring procedures of e-commerce platforms, they have ignored the more effective tools that are available in plain sight in China's legal system. By using these tools created by China's obsessive need to closely monitor and control all aspects of its civil society, brand owners can help to deter counterfeiters by forcing them to shed their concealment and anonymity and by exposing them to what they fear and loathe the most: transparency and accountability for their illegal actions.

V. APPENDICES

Appendix 1. Alibaba Listing: Gucci Guccio Handbags

Appendix 2. Alibaba Listing: Hennessy XO

Appendix 3. Alibaba Listing: Abercrombie & Fitch Sweatpants

Appendix 4. Abercrombie & Fitch Sweatpants

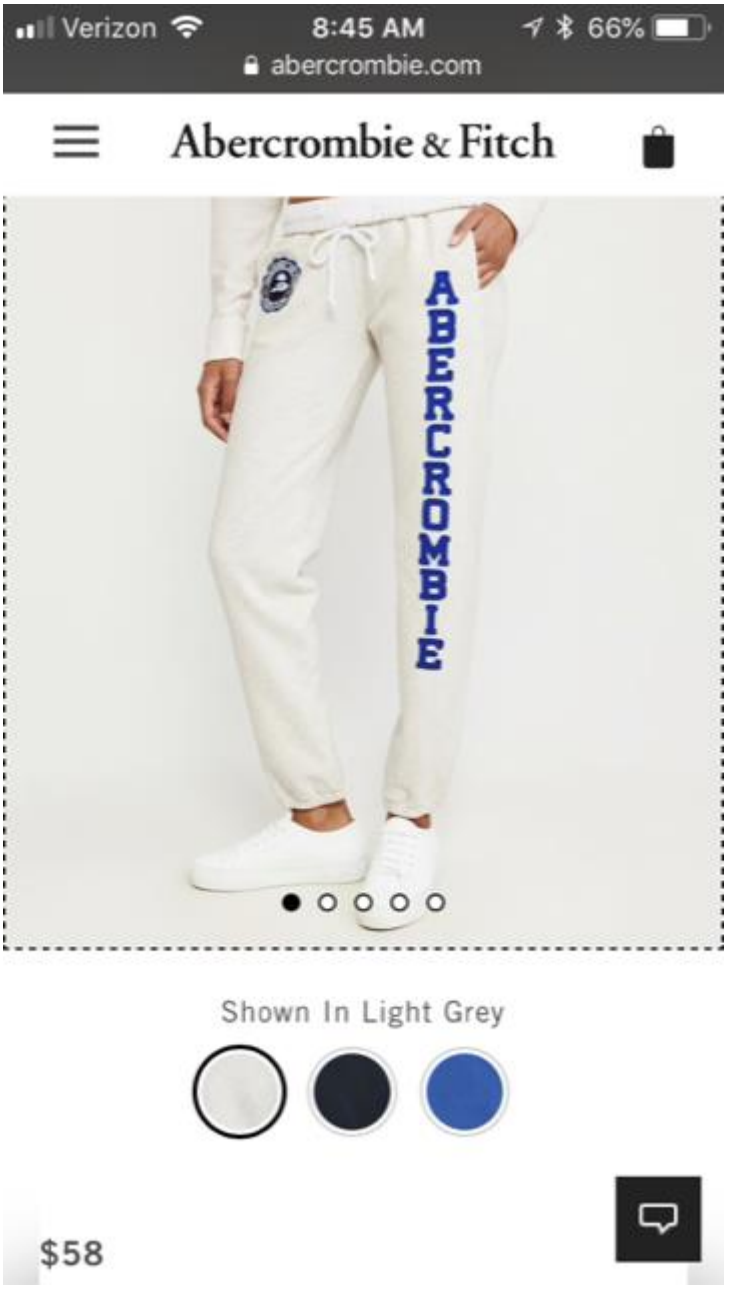


EXHIBIT 3

Combating Trafficking in Counterfeit and Pirated Goods

Report to the President of the United States

January 24, 2020

Homeland Security

Office of Strategy, Policy & Plans

Table of Contents

Table of Contents 2
1. Executive Summary 4
2. Introduction 7
3. Overview of Counterfeit and Pirated Goods Trafficking 10
4. Health and Safety, Economic, and National Security Risks 16
5. How E-Commerce Facilitates Counterfeit Trafficking 20
6. Private Sector Outreach and Public Comment 24
7. Immediate Action by DHS and Recommendations for the USG 26
8. Private Sector Best Practices 34
9. Conclusions 41
10. Appendix A: The IPR Center 42
11. Appendix B: Ongoing CBP Activities to Combat Counterfeit Trafficking 44
12. Appendix C: Homeland Security Investigations 47
13. Appendix D: U.S. Government Efforts 49
14. Appendix E: Global Initiatives 52
15. References 54

Foreword/Message from the Acting Secretary of Homeland Security

The rapid growth of e-commerce has revolutionized the way goods are bought and sold, allowing for counterfeit and pirated goods to flood our borders and penetrate our communities and homes. Illicit goods trafficked to American consumers by e-commerce platforms and online third-party marketplaces threaten public health and safety, as well as national security. This illicit activity impacts American innovation and erodes the competitiveness of U.S. manufacturers and workers.

Consumers must be confident in the safety, quality, and authenticity of the products they purchase online. DHS is committed to combating counterfeiters and pirates with the help of our U.S. Government partners and private sector stakeholders - who are critical to helping secure supply chains to stem the tide of counterfeit and pirated goods.

"Combating Trafficking in Counterfeit and Pirated Goods," has been prepared by the U.S. Department of Homeland Security's Office of Strategy, Policy, and Plans. The report uses available data, substantial public input, and other information to develop a deeper understanding of how e-commerce platforms, online third-party marketplaces, and other third-party intermediaries facilitate the importation and sale of massive amounts of counterfeit and pirated goods. The report identifies appropriate administrative, statutory, regulatory, and other actions, including enhanced enforcement measures, modernization of legal and liability frameworks, and best practices for private sector stakeholders. These strong actions can be implemented swiftly to substantially reduce trafficking in counterfeit and pirated goods while promoting a safer America.

This report was prepared pursuant to President Donald J. Trump's April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods*. The President's historic memorandum provides a much warranted and long overdue call to action in the U.S. Government's fight against a massive form of illicit trade that is inflicting significant harm on American consumers and businesses. This illicit trade must be stopped in its tracks.

This report was prepared in coordination with the Secretaries of Commerce and State, the Attorney General, the Office of Management and Budget, the Intellectual Property Enforcement Coordinator, the United States Trade Representative, the Assistant to the President for Economic Policy, the Assistant to the President for Trade and Manufacturing Policy, and with other partners in the U.S. Government. The report also benefitted from extensive engagement with the private sector.

Sincerely,

Chad Wolf
Acting Secretary,
U.S. Department of Homeland Security

1. Executive Summary

The President's April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods* calls prompt attention to illicit trade that erodes U.S. economic competitiveness and catalyzes compounding threats to national security and public safety.

Counterfeiting is no longer confined to street-corners and flea markets. The problem has intensified to staggering levels, as shown by a recent Organisation for Economic Cooperation and Development (OECD) report, which details a 154 percent increase in counterfeits traded internationally — from $200 billion in 2005 to $509 billion in 2016. Similar information collected by the U.S. Department of Homeland Security (DHS) between 2000 and 2018 shows that seizures of infringing goods at U.S. borders have increased 10-fold, from 3,244 seizures per year to 33,810.

Relevant to the President's inquiry into the linkages between e-commerce and counterfeiting, OECD reports that "E-commerce platforms represent ideal storefronts for counterfeits and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers."[1] Similarly, the U.S. Government Accountability Office (GAO) found that e-commerce has contributed to a shift in the sale of counterfeit goods in the United States, with consumers increasingly purchasing goods online and counterfeiters producing a wider variety of goods that may be sold on websites alongside authentic products.

Respondents to the July 10, 2019, Federal Register Notice issued by the Department of Commerce echoed these observations.[2] Perhaps most notably, the International Anti-Counterfeiting Coalition (IACC) reports that the trafficking of counterfeit and pirated goods in e-commerce is a top priority for every sector of its membership — comprised of more than 200 corporations, including many of the world's best-known brands in the apparel, automotive, electronics, entertainment, luxury goods, pharmaceutical, personal care and software sectors. The IACC submission goes on to say:

> *Across every sector of the IACC's membership, the need to address the trafficking of counterfeit and pirated goods in e-commerce has been cited as a top priority. The vast amounts of resources our members must dedicate to ensuring the safety and vitality of the online marketplace, bears out the truth of the issue highlighted by Peter Navarro, Assistant to the President for Trade and Manufacturing Policy, in his April 3, 2019 Op-Ed piece in The Wall Street Journal - that the sale of counterfeit brand-name goods presents a pervasive and ever-growing threat in the online space. One IACC member reported making*

[1] OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/9789264291652-en.

[2] Under Federal Register Notice (84 FR 32861), the Department of Commerce sought "comments from intellectual property rights holders, online third-party marketplaces and other third-party intermediaries, and other private-sector stakeholders on the state of counterfeit and pirated goods trafficking through online third-party marketplaces and recommendations for curbing the trafficking in such counterfeit and pirated goods."

hundreds of investigative online test purchases over the past year, with a nearly 80% successfully resulting in the receipt of a counterfeit item.[3]

The scale of counterfeit activity online is evidenced as well by the significant efforts e-commerce platforms themselves have had to undertake. A major e-commerce platform reports that its proactive efforts prevented over 1 million suspected bad actors from publishing a single product for sale through its platform and blocked over 3 billion suspected counterfeit listings from being published to their marketplace. Despite efforts such as these, private sector actions have not been sufficient to prevent the importation and sale of a wide variety and large volume of counterfeit and pirated goods to the American public.

The projected growth of e-commerce fuels mounting fears that the scale of the problem will only increase, especially under a business-as-usual scenario. Consequently, an effective and meaningful response to the President's memorandum is a matter of national import.

Actions to be Taken by DHS and the U.S. Government

Despite public and private efforts to-date, the online availability of counterfeit and pirated goods continues to increase. Strong government action is necessary to fundamentally realign incentive structures and thereby encourage the private sector to increase self-policing efforts and focus more innovation and expertise on this vital problem. Therefore, DHS will immediately undertake the following actions and make recommendations for other departments and agencies to combat the trafficking of counterfeit and pirated goods.

Immediate Actions by DHS and Recommendations for the U.S. Government
1. Ensure Entities with Financial Interests in Imports Bear Responsibility
2. Increase Scrutiny of Section 321 Environment
3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts
4. Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products
5. Leverage Advance Electronic Data for Mail Mode
6. Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION) Plan
7. Analyze Enforcement Resources
8. Create Modernized E-Commerce Enforcement Framework
9. Assess Contributory Trademark Infringement Liability for Platforms
10. Re-Examine the Legal Framework Surrounding Non-Resident Importers
11. Establish a National Consumer Awareness Campaign

[3] International Anti-Counterfeiting Coalition's comments made on the Department of Commerce, International Trade Administration, Office of Intellectual Property Rights', Report on the State of Counterfeit and Pirated Goods Trafficking Recommendations, 29 July 2019. Posted on 6 August 2019. https://www.regulations.gov/document?D=DOC-2019-0003-0072

Best Practices for E-Commerce Platforms and Third-Party Marketplaces

Government action alone is not enough to bring about the needed paradigm shift and ultimately stem the tide of counterfeit and pirated goods. All relevant private-sector stakeholders have critical roles to play and must adopt identified best practices, while redoubling efforts to police their own businesses and supply chains.

While the U.S. brick-and-mortar retail store economy has a well-developed regime for licensing, monitoring, and otherwise ensuring the protections of intellectual property rights (IPR), a comparable regime is largely non-existent for international e-commerce sellers. The following table catalogs a set of high priority "best practices" that shall be communicated to all relevant private sector stakeholders by the National Intellectual Property Rights Coordination Center. It shall be the Center's duty to monitor and report on the adoption of these best practices within the scope of the legal authority of DHS and the Federal government.

Best Practices for E-Commerce Platforms and Third-Party Marketplaces
1. Comprehensive "Terms of Service" Agreements
2. Significantly Enhanced Vetting of Third-Party Sellers
3. Limitations on High Risk Products
4. Rapid Notice and Takedown Procedures
5. Enhanced Post-Discovery Actions
6. Indemnity Requirements for Foreign Sellers
7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests for Information (RFI)
8. Pre-Sale Identification of Third-Party Sellers
9. Establish Marketplace Seller ID
10. Clearly Identifiable Country of Origin Disclosures

Foremost among these best practices is the idea that e-commerce platforms, online third-party marketplaces, and other third-party intermediaries such as customs brokers and express consignment carriers must take a more active role in monitoring, detecting, and preventing trafficking in counterfeit and pirated goods.

2. Introduction

> *E-commerce platforms represent ideal storefronts for counterfeits…and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers.*
>
> **- Organisation for Economic Cooperation and Development**[4]

The rapid growth of e-commerce platforms, further catalyzed by third-party online marketplaces connected to the platforms, has revolutionized the way products are bought and sold. "Online third-party marketplace" means any web-based platform that includes features primarily designed for arranging the sale, purchase, payment, or shipping of goods, or that enables sellers not directly affiliated with an operator of such platforms to sell physical goods to consumers located in the United States.

In the United States, e-commerce year-over-year retail sales grew by 13.3 percent in the second quarter of 2019 while total retail sales increased by only 3.2 percent as brick-and-mortar retail continued its relative decline.[5] For example, Amazon reports third-party sales on its marketplace grew from $100 million in 1999 to $160 *billion* in 2018.[6] In 2018 alone, Walmart experienced an e-commerce sales increase of 40 percent.[7]

Counterfeits threaten national security and public safety directly when introduced into government and critical infrastructure supply chains, and indirectly if used to generate revenue for transnational criminal organizations. Counterfeits also pose risks to human health and safety, erode U.S. economic competitiveness and diminish the reputations and trustworthiness of U.S. products and producers. Across all sectors of the economy, counterfeit goods unfairly compete with legitimate products and reduce the incentives to innovate, both in the United States and abroad.

While the expansion of e-commerce has led to greater trade facilitation, its overall growth—especially the growth of certain related business models—has facilitated online trafficking in counterfeit and pirated goods. American consumers shopping on e-commerce platforms and online third-party marketplaces now face a significant risk of purchasing counterfeit or pirated goods. This risk continues to rise despite current efforts across e-commerce supply chains to reduce such trafficking.

---

[4] OECD (2018), *Governance Frameworks to Counter Illicit Trade*, Illicit Trade, OECD Publishing, Paris, https://doi.org/10.1787/9789264291652-en.

[5] Department of Commerce, U.S. Census Bureau, Economic Indicators Division, "Quarterly Retail E-Commerce Sales 2nd Quarter 2019," 19 August 2019. https://www2.census.gov/retail/releases/historical/ecomm/19q2.pdf

[6] Jeff Bezos, "2018 Letter to Shareholders," *The Amazon Blog*. 11 April 2019. https://blog.aboutamazon.com/company-news/2018-letter-to-shareholders

[7] Note: Walmart does not separate out the percentage of third-party vendor sales. More information can be found, *here*, Jaiswal, Abhishek, "Getting Started Selling on Walmart in 2019: An Insider's Guide to Success," *BigCommerce*. https://www.bigcommerce.com/blog/selling-on-walmart-marketplace/#millennials-are-the-drivers-of-legacy-brand-change-including-walmart. *See also*, "Walmart Marketplace: Frequently Asked Questions," *Walmart.* https://marketplace.walmart.com/resources/#1525808821038-8edf332b-5ba2.

The OECD reports international trade in counterfeit and pirated goods amounted to as much as $509 billion in 2016. This represents a 3.3 percent increase from 2013 as a proportion of world trade. From 2003[8] through 2018, seizures of infringing goods by the U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) increased from 6,500 to 33,810 while the domestic value of seized merchandise — as measured by manufacturer's suggested retail price of the legitimate good (MSRP) — increased from $94 million in 2003 to $1.4 billion in 2018.[9]

The rise in consumer use of third-party marketplaces significantly increases the risks and uncertainty for U.S. producers when creating new products. It is no longer enough for a small business to develop a product with significant local consumer demand and then use that revenue to grow the business regionally, nationally, and internationally with the brand protection efforts expanding in step. Instead, with the international scope of e-commerce platforms, once a small business exposes itself to the benefits of placing products online — which creates a geographic scope far greater than its more limited brand protection efforts can handle — it begins to face increased foreign infringement threat.

Moreover, as costs to enter the online market have come down, such market entry is happening earlier and earlier in the product cycle, further enhancing risk. If a new product is a success, counterfeiters will attempt, often immediately, to outcompete the original seller with lower-cost counterfeit and pirated versions while avoiding the initial investment into research and design.

In other words, on these platforms, the counterfeit and pirated goods compete unfairly and fraudulently against the genuine items. While counterfeit and pirated goods have been sold for years on street corners, alleys, and from the trunks of cars, these illicit goods are now marketed to consumers in their homes through increasingly mainstream e-commerce platforms and third party online marketplaces that convey an air of legitimacy.

With the rise of e-commerce, the problem of counterfeit trafficking has intensified. The OECD documents a 154 percent increase in counterfeits traded internationally, from $200 billion in 2005 to $509 billion in 2016.[10] Data collected by CBP between 2000 and 2018 shows that seizures of infringing goods at U.S. borders, much of it trafficked through e-commerce, has increased ten-fold. Over 85 percent of the contraband seized by CBP arrived from China and Hong Kong. These high rates of seizures are consistent with a key OECD finding.

> *Counterfeit and pirated products come from many economies, with China appearing as the single largest producing market. These illegal products are frequently found in a range of industries, from luxury items (e.g. fashion apparel or deluxe watches), via intermediary products (such as machines, spare parts or*

[8] https://www.cbp.gov/sites/default/files/documents/FY2003%20IPR%20Seizure%20Statistics_0.pdf.
[9] https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf
[10] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147

chemicals) to consumer goods that have an impact on personal health and safety (such as pharmaceuticals, food and drink, medical equipment, or toys).[11]

Operation Mega Flex

In 2019, in response to the alarmingly high rates of contraband uncovered by DHS and a request from the White House Office of Trade and Manufacturing Policy (OTMP), CBP initiated Operation Mega Flex. This operation uses enhanced inspection and monitoring efforts to identify high-risk violators that are shipping and receiving illicit contraband through international mail facilities and express consignment hubs.

The periodic "blitz operations" conducted under the auspices of Operation Mega Flex examine thousands of parcels from China and Hong Kong and carefully catalog the range of contraband seized. To date, such operations have included visits to seven of CBP's international mail facilities and four express consignment hubs and the completion of over 20,000 additional inspections. The following table summarizes the findings of three Mega Flex blitzes conducted between July and September of 2019.

Results of Operation Mega Flex (2019)				
	Blitz I *July 16 & 17*	Blitz II *August 21*	Blitz III *September 18*	Total
Inspections	9,705	5,757	5,399	20,861
Discrepancies	1,145	1,010	735	2,890
Discrepancy Rate	11.8%	17.5%	13.6%	13.9%
Counterfeits	212	467	382	1,061
Counterfeit Rate	2.2%	8.1%	7.1%	5.1%

Source: U.S. Customs and Border Protection

Among the discrepancies uncovered by Operation Mega Flex were 1,061 shipments of counterfeit products. These counterfeits range from fake name brand items, like Louis Vuitton bags to sports equipment made with faulty parts. Other contraband included drug paraphernalia, deadly opioids, and counterfeit drivers' licenses.[12] In all, counterfeits constituted more than one of every three discrepancies uncovered by inspectors.[13]

---

[11] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. https://www.oecd-ilibrary.org/docserver/9789264252653-en.pdf?expires=1576509401&id=id&accname=id5723&checksum=576BF246D4E50234EAF5E8EDF7F08147

[12] Oren Fliegelman, "Made in China: Fake IDs," *The New York Times.* 6 February 2015. https://www.nytimes.com/2015/02/08/education/edlife/fake-ids-or-why-would-a-student-order-a-tea-set.html

[13] Among the near 3,000 discrepancies, 20% of them were agricultural violations, such as bad meat, fruit, or produce, unsafe for the American consumer. These agricultural discrepancies are dangerous to the United States because they may contain diseases or pests that can greatly impact agriculture. For example, on October 16, 2018, CBP seized nearly 900 pounds of mitten crabs from an incoming Chinese freight. In Asia, mitten crabs are considered a seasonal delicacy; however, they have a disastrous impact on other global habitats and are labeled as an invasive species. See, Department of Homeland Security, U.S. Customs and Border Protection, "CBP Prevents Smuggling of Nearly 900 Pounds of Invasive Mitten Crabs," 31 October 2018. https://www.cbp.gov/newsroom/national-media-release/cbp-prevents-smuggling-nearly-900-pounds-invasive-mitten-crabs.

Authorities also seized 174 controlled or prohibited substances, including: recreational drugs like LSD, cocaine, DMT, ecstasy, marijuana, mushrooms, and poppy pods as well as steroids and highly addictive painkillers like Tramadol.

It is not just a rise in the volume of counterfeits we are witnessing. GAO notes that counterfeiters are increasingly producing a "wider variety of goods that may be sold on websites alongside authentic products."[14]

DHS finds the current state of e-commerce to be an intolerable and dangerous situation that must be addressed firmly and swiftly by strong actions within the Department and across other relevant agencies of the U.S. Government (USG). These include: The Federal Bureau of Investigation and the Department of Justice, the Department of Commerce, and the Department of the Treasury. This report provides a blueprint for swift and constructive changes and sets forth several actions for immediate implementation.

3. Overview of Counterfeit and Pirated Goods Trafficking

While most e-commerce transactions involve legitimate sellers and products, far too many involve the trafficking of counterfeit and pirated goods and expose legitimate businesses and consumers to substantial risks. This is a global phenomenon; the OECD reports international trade in counterfeit and pirated goods amounted to as much as half a trillion dollars in 2016.[15]

Key Drivers of Counterfeiting and Piracy in E-Commerce

Historically, many counterfeits were distributed through swap meets and individual sellers located on street corners. Today, counterfeits are being trafficked through vast e-commerce supply chains in concert with marketing, sales, and distribution networks. The ability of e-commerce platforms to aggregate information and reduce transportation and search costs for consumers provides a big advantage over brick-and-mortar retailers. Because of this, sellers on digital platforms have consumer visibility well beyond the seller's natural geographical sales area.

Selling counterfeit and pirated goods through e-commerce is a highly profitable activity: production costs are low, millions of potential customers are available online, transactions are convenient, and listing on well-branded e-commerce platforms provides an air of legitimacy.

Other discrepancies found by CBP in the blitz operations included 13 weapon modifications and gun parts, 3 occurrences of drug paraphernalia, and 3 pill presses. For full summary of findings, see, Department of Homeland Security, U.S. Customs and Border Protection, Operation Mega Flex I, II and III Summaries, 2019.

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

[15]See OECD, Trends in Trade in Counterfeit and Pirated Goods (March 2019), available at https://www.oecd.org/governance/risk/trends-in-trade-in-counterfeit-and-pirated-goods-g2g9f533-en.htm

[15]See Parker et al. 2016

When sellers of illicit goods are in another country, they are largely outside the jurisdiction for criminal prosecution or civil liability from U.S. law enforcement and private parties.

The Role of Online Third-Party Marketplaces

Third-party online marketplaces can quickly and easily establish attractive "store-fronts" to compete with legitimate businesses. On some platforms, little identifying information is necessary to begin selling.

A counterfeiter seeking to distribute fake products will typically set up one or more accounts on online third-party marketplaces. The ability to rapidly proliferate third-party online marketplaces greatly complicates enforcement efforts, especially for intellectual property rights holders. Rapid proliferation also allows counterfeiters to hop from one profile to the next even if the original site is taken down or blocked. On these sites, online counterfeiters can misrepresent products by posting pictures of authentic goods while simultaneously selling and shipping counterfeit versions.

Counterfeiters have taken full advantage of the aura of authenticity and trust that online platforms provide. While e-commerce has supported the launch of thousands of legitimate businesses, their models have also enabled counterfeiters to easily establish attractive "store-fronts" to compete with legitimate businesses.

Platforms use their third-party marketplace functions to leverage "two-sided" network effects to increase profitability for the platform by adding both more sellers and more buyers. Because sellers benefit with each additional buyer using the platform (more consumers to sell to), and buyers are more likely to join/use the platform with each additional seller (more sellers to buy from), there can be diminished internal resistance to adding lower quality sellers.

Platforms that recognize this strategy may incentivize seller listings to stimulate further growth and increase profits but do so without adequate scrutiny. As just one incentive, many platforms create "frictionless entry" by reducing the costs for sellers and buyers to join, thereby increasing the likelihood that the platform will reach an efficient and highly profitable scale.

Platforms also generate value by opening previously unused (or less frequently used) markets. In addition, online platforms reduce transaction costs by streamlining the actual transaction; for example, buyers and sellers use a standardized transaction method that simplifies interactions with buyers and reduces the risk that the buyer will not pay.

For example, before the rise of e-commerce, secondhand products could be sold at garage sales or in classified newspaper advertisements. E-commerce created a process for allowing buyers and sellers to trade goods digitally, reducing transaction costs and creating a global marketplace for used, but too often counterfeit, products.

Another way platforms generate value is by aggregating information and reducing search costs. A buyer may search for a product, either by keyword or product category, at lower search cost than visiting brick-and-mortar stores. Because of this, sellers on digital platforms have consumer visibility well beyond the seller's natural geographical sales area.

In addition, consumers who have made a purchase may use tools provided by the marketplace to rate the product and the seller involved. These ratings create an important mechanism to facilitate future consumer trust in an otherwise unknown seller.

In principle, such a rating system provides a key to overcoming a common economic problem that might otherwise preclude sales: without a low-cost trust building feature that also communicates quality, and in a market with significant numbers of low-quality products, buyers may refuse to purchase any product at all, or would demand a lower price to reflect the uncertainty. One frequent result is that low cost counterfeits drive out high quality, trusted brands from the online marketplace. In practice, even the ratings systems across platforms have been gamed, and the proliferation of fake reviews and counterfeit goods on third-party marketplaces now threatens the trust mechanism itself.

Lower Startup and Production Costs

The relative ease of setting up and maintaining e-commerce websites makes online marketplaces a prime locale for the retailing of counterfeit and pirated goods. E-commerce retailers enjoy low fixed costs of setting up and maintaining web businesses and lower costs for carrying out normal business operations such as managing merchant accounts. These ventures can be set up quickly without much sophistication or specialized skills.

Some online platforms allow retailers to use pre-made templates to create their stores while other platforms only require that a seller create an account. These businesses face much lower overhead costs than traditional brick-and-mortar sellers because there is no need to rent retail space or to hire in-person customer-facing staff. Not only can counterfeiters set up their virtual storefronts quickly and easily, but they can also set up new virtual storefronts when their existing storefronts are shut down by either law enforcement or through voluntary initiatives set up by other stakeholders such as market platforms, advertisers, or payment processors.

In the production stage, counterfeiters keep costs low by stealing product secrets or technological knowledge, exploiting new production technologies, and distributing operations across jurisdictions. One method involves employees who sell trade secrets to a third party who, in turn, develops and sells counterfeit products based on the stolen secrets. Another method relies on an intermediary to steal a firm's product or technology. The use of intermediaries reduces the traceability to the counterfeiter.

Counterfeiting and piracy operations also take advantage of new low-cost production technologies. For example, the technological advances in modeling, printing and scanning technologies such as 3D printing reduce the barriers for reverse engineering and the costs of manufacturing counterfeit products.

Lower production costs can also be achieved through distributed production operations. One method involves manufacturing the counterfeit good in a foreign market to lower the chances of detection and to minimize legal liability if prosecuted. This can be combined with importation of

the counterfeit labels separately from the items, with the labels being applied to the products after both items arrive in the U.S.

In addition, it is much cheaper to manufacture illicit goods because counterfeit and pirated goods are often produced in unsafe workplaces with substandard and unsafe materials by workers who are often paid little—and sometimes nothing in the case of forced labor. Moreover, in the case of goods governed by Federal health and safety regulations, it often costs much less to produce counterfeit versions that do not meet these health and safety standards.

Lower Marketing Costs

Businesses that use only an internet presence as their consumer-facing aspect typically enjoy lower costs of designing, editing, and distributing marketing materials. Counterfeiters also benefit from greater anonymity on digital platforms and web sites and greater ease to retarget or remarket to customers. For example, counterfeiters use legitimate images and descriptions on online platforms to confuse customers, and they open multiple seller accounts on the platform so that if one account is identified and removed, the counterfeiter can simply use another.

The popularity of social media also helps reduce the costs of advertising counterfeit products. The nature of social media platforms has aided in the proliferation of counterfeits across all e-commerce sites. Instagram users, for example, can take advantage of connectivity algorithms by using the names of luxury brands in hashtags. Followers can search by hashtag and unwittingly find counterfeit products, which are comingled and difficult to differentiate from legitimate products and sellers.

Lower Distribution Costs

Traditionally, many counterfeit goods were distributed through swap meets and individual sellers located on street corners. With the rise of online platforms for shopping, customers can have products delivered to them directly.

Foreign entities that traffic in counterfeits understand how to leverage newer distribution methods better suited to e-commerce than the traditional trade paradigm (i.e., imports arriving via large cargo containers with domestic distribution networks). Today, mail parcel shipments, including through express consignments, account for more than 500 million packages each year.[16] Seizures in the small package environment made up 93 percent of all seizures in 2018, a 6 percent increase over 2017. From 2012 to 2016, the number of seizures from express consignment carriers increased by 105 percent, and the MSRP of those seizures had a 337 percent increase.[17] In contrast, seizures from cargo decreased by 36 percent from FY17 to FY18.

[16] https://www.cbp.gov/sites/default/files/assets/documents/2019-Apr/FY%202017%20Seizure%20Stats%20Booklet%20-%20508%20Compliant.pdf p. 14
[17] https://www.gao.gov/assets/690/689713.pdf?mod=article_inline p. 14

The International Chamber of Commerce found that counterfeiters use international air packages because the high volume of these packages makes enforcement more difficult.[18] A recent report by the OECD points out that distributing counterfeits across a series of small packages spreads the risk of detection, and lowers the loss from having one or more shipments seized, suggesting that losses to the counterfeiter on an ongoing basis would be within a tolerable range.[19]

The OECD report also notes that it is harder for authorities to detect counterfeits in small parcels than in shipping containers because cargo containers making entry at a maritime port provide customs officials with more information, well in advance of arrival. Moreover, the effort required for CBP to seize a shipment does not vary by size of the shipment, meaning that a package of a few infringing goods requires the same resources to seize as a cargo container with hundreds of infringing goods.

Section 321 of the Tariff Act of 1930 has likewise encouraged counterfeiters to favor smaller parcel delivery. Under Section 321, a foreign good valued at or less than $800 and imported by one person on one day is not subject to the same formal customs entry procedures and rigorous data requirements as higher-value packages entering the United States. This reduced level of scrutiny is an open invitation to exploit Section 321 rules to transport and distribute counterfeits.

Rules set by the Universal Postal Union (UPU) have historically contributed to the distortion in rates for delivery of international e-commerce purchases to the United States.[20] UPU reimbursement rates have underpriced domestic postage rates for small parcels. This market distortion made it cheaper for small package exports to the United States. from certain countries than would otherwise be economically feasible and has encouraged the use of the international postal mode over other shipment channels. The United States recently scored a historic victory when the UPU overhauled its terminal dues system[21], effectively eliminating this outdated policy.[22]

Consumer Attitudes and Perceptions

The sale of counterfeits away from so-called "underground" or secondary markets (e.g. street corners, flea markets) to e-commerce platforms is reshaping consumer attitudes and perceptions. Where in the past, consumers could identify products by relying on "red flag" indicators—such as a suspicious location of the seller, poor quality packaging, or discount pricing—consumers are now regularly exposed to counterfeit products in settings and under conditions where the articles appear genuine.

While the risks of receiving a counterfeit may have been obvious to a consumer purchasing items on street corners, with the rise of online platforms, it is not so obvious anymore. For example, it is

[18] https://cdn.iccwbo.org/content/uploads/sites/3/2015/03/ICC-BASCAP-Roles-and-Responsibilities-of-Intermediaries.pdf p. 32
[19] OECD/EUIPO (2018), *Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends, Illicit Trade*, OECD Publishing, Paris. https://doi.org/10.1787/9789264307858-en p. 77
[20] The UPU is a specialized agency of the United Nations that coordinates postal policies between 190 countries. Importantly, these treaties determine the cost of shipping between the various countries and offers low rates to mail originating from abroad, as compared to domestic postage rates.
[21] Universal Postal Union (2019), *Decisions of the 2019 Geneva Extraordinary Congress*, http://www.upu.int/uploads/tx_sbdownloader/actsActsOfTheExtraordinaryCongressGenevaEn.pdf
[22] https://www.nytimes.com/2019/09/25/business/universal-postal-union-withdraw.html

unlikely that anyone would set out to purchase a counterfeit bicycle helmet given the potential safety risks; however, such items are readily available to unsuspecting consumers on e-commerce websites.

Reports indicate that some third-party marketplace listings falsely claim to have certifications with health and safety standards or offer items banned by federal regulators or even the platforms themselves. Coupled with the inability of buyers to accurately determine the manufacturer or the origin of the product, it is challenging for buyers to make informed decisions in the e-commerce environment.

In 2017, MarkMonitor found that 39 percent of all unwitting purchases of counterfeit goods were bought through online third-party marketplaces.[23] Sellers on large well-known platforms rely on the trust that those platforms hosting of the marketplace elicits. The results of this survey indicate that bad actors selling counterfeit goods on legitimate online platforms erodes trust in both the brands and the platforms themselves.

In 2018, Incopro conducted a survey focusing on United Kingdom (UK) consumers who had unwittingly purchased counterfeit goods and how their perceptions of online marketplaces were affected as a result.[24] The results of this survey show that 26 percent of respondents reported that they had unwittingly purchased counterfeits. Of these, 41 percent reported that they had never received a refund after reporting a seller to online marketplaces.

In addition, roughly one-third of respondents reported that they would be less likely to buy a widely counterfeited product from an online marketplace while 46 percent reported no longer using a particular online marketplace after receiving counterfeit goods. Respondents also reported that, when trying to differentiate between genuine and counterfeit products, they consider online reviews along with the reputation of online marketplaces.

These recent findings, against the larger backdrop of the e-commerce environment, demonstrate the immediacy of the problem as consumer confidence and brand integrity continue to suffer in the realm of online third-party marketplaces.

Top Products Prone to Counterfeiting and Piracy

Counterfeiters sell fake goods as authentic goods — for example, a copy of a Louis Vuitton bag or Rolex watch fraudulently sold as the "real thing." Counterfeiters use identical copies of registered trademarks without the authorization of the rightful owner.

Piracy typically refers to the act of copying a protected work (such as a book, movie, or music) without the consent of the rights holder or person duly authorized by the rights holder.

[23]MarkMonitor (2017). *MarkMonitor Online Barometer: Global online shopping survey 2017 – consumer goods.* Downloaded from https://www.markmonitor.com/download/report/MarkMonitor_Online_Shopping_Report-2017-UK.pdf. p. 6
[24]INCOPRO, 2018. Counterfeit Products are Endemic – and it is damaging brand value: INCOPRO Market Research Report available at https://www.incoproip.com/cms/wp-content/uploads/2018/11/2018_Incopro_Market-Research-report.pdf.

The below table provides a summary of the annual IPR seizure statistics collected by CBP in FY18; including items from all modes of transportation. Apparel and other types of accessories, along with footwear, top the list at 18 percent and 14 percent of seizures, respectively. Commonly counterfeited items in these categories include brand name shoes such as Nike and Adidas, as well as NFL jerseys.

Watches and jewelry follow at 13 percent of total seizures. During the Mega Flex operation on August 21, 2019, for example, CBP officers seized counterfeit Rolex watches valued at over $1.4 million. Handbags and wallets represented nearly 11 percent of all seizures, including counterfeits of luxury brands such as Louis Vuitton, Michael Kors, and Gucci. Consumer electronics represented 10 percent of seizures, including products such as iPhones, hover boards, earbuds, microchips, and others.

Pharmaceuticals and personal care items account for only 7 percent of total seizures. However, as discussed in the next section, many of the products in these categories pose significant dangers to the consumer. Fake prescription drugs can lack active ingredients, contain incorrect dosages, or include dangerous additives. Fake personal care items such as cosmetics have been found to contain everything from harmful bacteria to human waste. Between 2017 and 2018, CBP and ICE Homeland Security Investigations (HSI) seized over $31 million in fake perfumes from China.

CBP Intellectual Property Rights Annual Seizure Statistics Fiscal Year 2018		
Products	**Seizures**	**Percent of Total**
1. Wearing Apparel/Accessories	6,098	18%
2. Footwear	4,728	14%
3. Watches/Jewelry	4,291	13%
4. Handbags/Wallets	3,593	11%
5. Consumer Electronics	3,388	10%
6. Consumer Products	2,816	8%
7. Pharmaceuticals/Personal Care	2,293	7%
8. Optical Media	561	2%
9. Toys	487	1%
10. Computers/Accessories	450	1%

Source: U.S. Customs and Border Protection

4. Health and Safety, Economic, and National Security Risks

Counterfeit trafficking exposes American consumers to significant health and safety risks — in addition to significant economic impacts and, in some cases, threats to national security.

Health and Safety

The types of counterfeit goods available on e-commerce platforms go far beyond those products with potential hidden toxins — like sports jerseys, jewelry and purses—and include many products

that can pose more obvious serious risks to health and safety, like prescription drugs and air bags. It is not only the sellers of the counterfeit goods, but also the e-commerce platforms and other third-party intermediaries (e.g., shippers) that facilitate their sale, that are profiting from the marketing and distribution of these illicit products to the American public.

The profit margins are especially high for counterfeiters in the sale of counterfeit pharmaceuticals. In the past, counterfeit prescription drugs primarily involved so-called lifestyle drugs like sildenafil (Viagra). Today, this market has expanded to include all types of therapeutic medicines, including insulin, cancer medications, and cardiovascular drugs.

Counterfeiting has also spread into over-the-counter medicines like cough syrup and weight loss drugs. As more Americans purchase drugs online, many U.S. consumers appear to be largely unaware of the potential dangers of purchasing counterfeit drugs from internet pharmacies.

Unlike legitimate drug manufacturers that are subject to inspections by the U.S. Food and Drug Administration, labs that manufacture counterfeits have no such oversight. According to a 2019 Better Business Bureau study, "companies based in China, Hong Kong, Singapore, and India shipped 97 percent of the counterfeit medicines seized in the U.S."[25]

In March 2019, Europol, the European Union's law enforcement agency, seized 13 million doses of counterfeit medicine ranging from opioids to heart medication. Europol noted that this type of counterfeiting is on the rise due to the relatively low risk of criminal detection.[26]

Counterfeit medicines not only defraud consumers who are often afflicted with serious health issues; they can also be lethal. Fake prescription opioids are often laced with deadly fentanyl, much of which originates in China. In raising awareness of the dangers, the National Institutes of Health (NIH) has warned:

> *Preventing counterfeit medicines from entering the United States is especially difficult, in part because nearly 40 percent of drugs are made overseas and approximately 80 percent of the active medicinal components of drugs are imported. Because many of these medicines are expensive, buyers are attracted by lower prices. The rise of Internet pharmacies makes regulation of drug safety more difficult.* [27]

---

[25]Baker, C. Steven, "Fakes are Not Fashionable: A BBB Study of the Epidemic of Counterfeit Goods Sold Online," *Better Business Bureau*, May 2019. https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf

[26]Baker, C. Steven, "Fakes are Not Fashionable: A BBB Study of the Epidemic of Counterfeit Goods Sold Online," *Better Business Bureau*, May 2019. Pg. 9. https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf

[27]National Institutes of Health, Blackstone, Erwin A., Joseph P. Fuhr Jr., and Steve Pociask, "The Health and Economic Effects of Counterfeit Drugs," *American Health and Drug Benefits* 7(4): 216-224, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4105729/; See also, Mackey, Tim K., et al., "After counterfeit Avastin®-- what have we learned and what can be done," *Nature Reviews Clinical Oncology* 12, 302-308. 2015. https://www.nature.com/articles/nrclinonc.2015.35.pdf

Health and safety risks extend far beyond fake prescription drugs. Counterfeit cosmetics often contain ingredients such as arsenic, mercury, aluminum, or lead and may be manufactured in unsanitary conditions, which can ultimately lead to problems with one's eyes or skin.

An investigation of counterfeit iPhone adapters conducted by the GAO found a 99 percent failure rate in 400 counterfeit adapters tested for safety, fire, and shock hazards, and found that 12 of the adapters posed a risk of lethal electrocution to the user.[28] In December 2015, CBP seized 1,378 hover boards with counterfeit batteries, which can cause fires resulting in injury or death.[29]

Children's toys, some laced with deadly metals like cadmium and lead, represent another area in which counterfeiters have taken advantage of e-commerce business models that provide limited to no accountability for sellers.

The Department of Justice has prosecuted individuals for the online sale of a "high value target" of counterfeiters — namely, airbags.[30] Along with other counterfeit automotive parts like brake pads, wheels, and seat belts, unsafe airbags can have catastrophic consequences for drivers, as well as for their passengers and others on the road. Bicycle helmets, another favorite of counterfeiters, likewise can lead to catastrophic consequences for cyclists.

Of the contraband products seized in 2016 by CBP and ICE/HSI, an astonishing 16 percent posed direct and obvious threats to health and safety.[31] E-commerce also facilitates the widespread sale of pirated versions of copyrighted works. Pirated medical books — which can contain errors that endanger patients' lives — have been found on platforms along with other pirated books (textbooks and trade books) and illicit reproductions of music-CD box sets.

Economic Harm

The growth in online sales of counterfeit and pirated goods directly harms — and unfairly competes against — the many legitimate companies that produce, sell and distribute genuine goods, often resulting in lost profits, employee layoffs, and diminished incentives to innovate. Frontier Economics (2018) finds that counterfeit goods displaced roughly half a trillion dollars of global sales of legitimate companies in 2013 and forecasts this displacement to reach $1 to $1.2 trillion by 2022.[32] The study also estimates that global employment losses due to counterfeit goods

[28]Underwriters Laboratory (UL), "Counterfeit iPhone Adapters", available at: https://legacy-uploads.ul.com/wp-content/uploads/sites/40/2016/09/10314-CounterfeitiPhone-WP-HighRes_FINAL.pdf. Also *see*, U.S. Government Accountability Office Report to the Chairman, Committee on Finance, U.S. Senate: *Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market*, GAO-18-216, Washington, DC: Government Accountability Office, January 2018. Pg.18. https://www.gao.gov/assets/690/689713.pdf

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

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

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

[32]https://iccwbo.org/publication/economic-impacts-counterfeiting-piracy-report-prepared-bascap-inta/

were between 2 million and 2.6 million jobs in 2013, with job displacement expected to double by 2022.

Counterfeit goods also damage the value of legitimate brands. When brand owners lose the ability to collect a price premium for branded goods, it leads to diminished innovation as brand owners are less likely to invest in creating innovative products. Legitimate companies, and particularly small businesses, report devastating impacts due to the abundance of competing online counterfeits and pirated goods. Moreover, while e-commerce platforms can benefit legitimate businesses by helping them to reach customers with a new product, the same process and technology also makes it easier for unscrupulous firms to identify popular new products, produce infringing versions of them, and sell these illicit goods to the business's potential customers.

As previously noted, the speed at which counterfeiters can steal intellectual property through e-commerce can be very rapid. If a new product is a success, counterfeiters may attempt to immediately outcompete the original seller with lower-cost counterfeit versions — while avoiding research and development costs. The result: counterfeiters may have a significant competitive advantage in a very short period of time over those who sell trusted brands.

Such fast-track counterfeiting poses unique and serious problems for small businesses, which do not have the same financial resources as major brands to protect their intellectual property. Lacking the ability to invest in brand-protection activities, such as continually monitoring e-commerce platforms to identify illicit goods, perform test buys, and send takedown notices to the platforms, smaller businesses are more likely to experience revenue losses as customers purchase counterfeit versions of the branded products.

In many cases, American enterprises have little recourse aside from initiating legal action against a particular vendor. Such legal action can be extremely difficult. Many e-commerce sellers of infringing products are located outside the jurisdiction of the United States, often in China; existing laws and regulations largely shield foreign counterfeiters from any accountability.

Organized Crime and Terrorism

The impact of counterfeit and pirated goods is broader than just unfair competition. Law enforcement officials have uncovered intricate links between the sale of counterfeit goods and transnational organized crime. A study by the Better Business Bureau notes that the financial operations supporting counterfeit goods typically require central coordination, making these activities attractive for organized crime, with groups such as the Mafia and the Japanese Yakuza heavily involved.[33] Criminal organizations use coerced and child labor to manufacture and sell counterfeit goods. In some cases, the proceeds from counterfeit sales may be supporting terrorism and dictatorships throughout the world.[34]

[33]https://www.bbb.org/globalassets/local-bbbs/st-louis-mo-142/st_louis_mo_142/studies/counterfeit-goods/BBB-Study-of-Counterfeit-Goods-Sold-Online.pdf

[34]United Nations Office of Drugs and Crime (UNODC), *Focus On: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime*, available at: https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf

National Security

One of the greatest threats counterfeits pose to national security is their entry into the supply chain of America's defense industrial base. This defense industrial base includes both private sector contractors and government agencies, particularly the Department of Defense.

In FY 2018, 12 percent of DHS seizures included counterfeit versions of critical technological components, automotive and aerospace parts, batteries, and machinery. Each of these industrial sectors have been identified as critical to the defense industrial base, and thus critical to national security. One example drawn from a 2018 study by the Bureau of Industry and Security within the Department of Commerce featured the import of counterfeit semiconductors or "Trojan chips" for use in defense manufacturing and operations[35]. Such Trojan chips can carry viruses or malware that infiltrate and weaken American national security. The problem of counterfeit chips has become so pervasive that the Department of Defense has referred to it as an "invasion." Companies from China are the primary producers of counterfeit electronics.[36]

5. How E-Commerce Facilitates Counterfeit Trafficking

While e-commerce has supported the launch of thousands of legitimate businesses, e-commerce platforms, third-party marketplaces, and their supporting intermediaries have also served as powerful stimulants for the trafficking of counterfeit and pirated goods. The central economic driver of such trafficking is this basic reality: Selling counterfeit and pirated goods through e-commerce platforms and related online third-party marketplaces is a highly profitable venture.

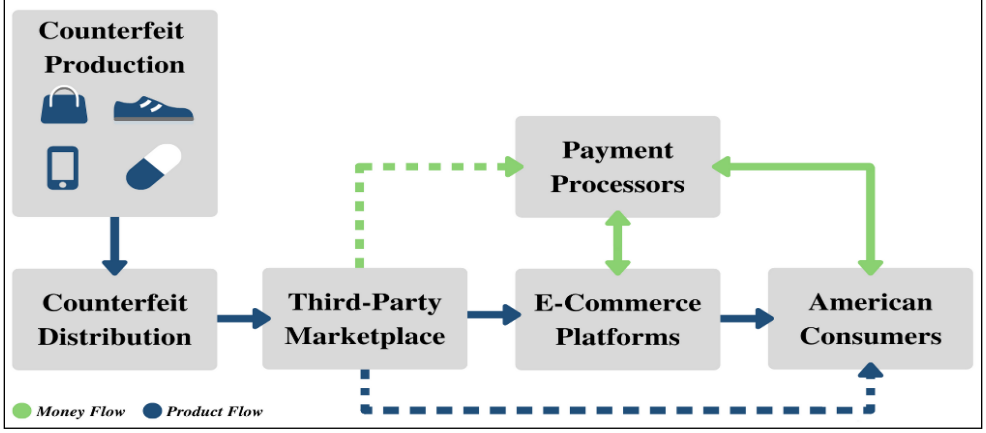
For counterfeiters, production costs are low, millions of potential customers are available online, transactions are convenient, and listing goods on well-known platforms provides an air of legitimacy. When sellers of illicit goods are in another country, they are also exposed to relatively little risk of criminal prosecution or civil liability under current law enforcement and regulatory practices. It is critical that immediate action be taken to protect American consumers and other stakeholders against the harm and losses inflicted by counterfeiters.

[35] https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

[36] Saunders, Gregory and Tim Koczanksi, "Counterfeits," *Defense Standardization Program Journal*, October/December 2013. https://www.dsp.dla.mil/Portals/26/Documents/Publications/Journal/131001-DSPJ.pdf

Figure One provides a simplified overview of how counterfeit products move from production by counterfeiters to sales to American consumers:

Figure One: Counterfeit Production to Sales in the E-Commerce Paradigm



Counterfeit Production and Distribution

The counterfeit sales process begins with some type of production capability for the counterfeit good. In this stage, counterfeiters enjoy enormous production cost advantages relative to legitimate businesses. Counterfeits are often produced in unsafe workplaces, with substandard and unsafe materials, by workers who are often paid little or sometimes nothing in the case of forced labor.

In the case of goods subject to federal health and safety regulations, it costs much less to produce counterfeit versions that do not meet these health and safety requirements that make the legitimate products so safe.

Counterfeiters likewise minimize the need for incurring significant research and development expenditures by stealing intellectual property, technologies, and trade secrets. They also shave production costs using inferior ingredients or components.

For example, a common way for counterfeiters to produce *fake* prescription opioids like Oxycontin, or a prescription drug like Viagra, is to start with the *real* pills as a basic ingredient. These real pills are then ground up into a powder, diluted with some type of (sometimes toxic) powder filler, and then "spiked" with an illegal and deadly narcotic like fentanyl, in the case of fake opioids, or illegal and deadly amphetamines or strychnine, in the case of Viagra.

In the case of apparel, such as running shoes, employees from a legitimate branded company may leave the company and set up their own facility. These employees have the expertise to manufacture identical-looking shoes; but they will typically do so with cheaper, inferior components. The result: the shoes may fail during activity, injure the user with an inferior insole, or, at a minimum, wear out faster than the real product.[37]

[37]Department of Homeland Security, U.S. Customs and Border Protection, "CBP Seizes Over $2.2 Million worth of Fake Nike Shoes at LA/Long Beach Seaport," 9 October 2019. https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-over-22-million-worth-fake-nike-shoes-lalong-beach-seaport

The technological advances in modeling, printing, and scanning technologies such as 3D printing, have also significantly reduced the barriers for reverse engineering and the costs of manufacturing counterfeit products. Again, one problem that may arise may be the use of inferior production inputs that lead to product failure.

These are just a few of the many ways counterfeits begin their long journey into American households. There is often no way for legitimate businesses to compete, on a production cost basis, with counterfeiters. There is also often no way for a consumer to tell the difference between a counterfeit and legitimate good.

Third-Party Marketplaces and Counterfeiter Websites

A counterfeiter seeking to distribute fake products will typically set up one or more accounts on third-party marketplaces, and these accounts can often be set up quickly and without much sophistication or many specialized skills. Under such circumstances, it is axiomatic that online retailers face much lower overhead costs than traditional brick-and-mortar sellers. There is no need to rent retail space or to hire in-person, customer-facing staff.

In a common scenario, third-party marketplace websites contain photos of the real product, fake reviews of the counterfeit product, and other such disinformation designed to mislead or fool the consumer into believing the legitimacy of the product. The proliferation of such disinformation is the hallmark of the successful online counterfeiter. Such deception not only provides counterfeiters with an enormous competitive advantage over their brick-and-mortar counterparts; legitimate sellers on the internet are harmed as well.

In some cases, counterfeiters hedge against the risk of being caught and their websites taken down from an e-commerce platform by preemptively establishing multiple virtual store-fronts. A key underlying problem here is that on at least some e-commerce platforms, little identifying information is necessary for a counterfeiter to begin selling. In the absence of full transparency, counterfeiters can quickly and easily move to a new virtual store if their original third-party marketplace is taken down.

The popularity of social media also helps proliferate counterfeits across various e-commerce platforms. Instagram users, for example, can take advantage of connectivity algorithms by using the names of luxury brands in hashtags. Followers can search by hashtag and unwittingly find counterfeit products, which are comingled and difficult to differentiate from legitimate products and sellers.

According to a 2019 report, *Instagram and Counterfeiting*, nearly 20 percent of the posts analyzed about fashion products on Instagram featured counterfeit or illicit products.[38] More than 50,000 Instagram accounts were identified as promoting and selling counterfeits, a 171 percent increase from a prior 2016 analysis. Instagram's Story feature, where content disappears in twenty-four hours, was singled out as particularly effective for counterfeit sellers.

[38]Stroppa, Andrea*, et al*., "Instagram and counterfeiting in 2019: new features, old problems," *Ghost Data*, 9 April 2019. Rome, New York. https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf

A more recent development on social media is the proliferation of "hidden listings" for the sale of counterfeits. Social media is used to provide direct hyperlinks in private groups or chats to listings for counterfeit goods that purport to be selling unrelated legitimate items. By accessing the link, buyers are brought to an e-commerce platform which advertises an unrelated legitimate item for the same price as the counterfeit item identified in the private group or chat. The buyer is directed to purchase the unrelated item in the listing but will receive the sought-after counterfeit item instead.

Order Fulfillment in E-Commerce

The foreign counterfeiter must first choose between sending a package either by express consignment carrier or through the international post. As a general proposition, express consignment shippers — such as DHL Express, Federal Express, and the United Parcel Service — were subject to data requirements before they were extended to the international posts.

In the next step along the delivery chain, a parcel will arrive at a port of entry under the authority of CBP. Millions of parcels arrive daily, and it is impossible to inspect more than a very small fraction.

Although ocean shipping is still a major mode of transport for counterfeits, the rapid growth of other modes, such as truck and air parcel delivery, threaten to upend established enforcement efforts, and as such, is increasingly used by international counterfeiters. This continued shift from bulk cargo delivery to other modes by counterfeiters is illustrated in the trends in seizure statistics.

It is clear from these observations that counterfeit traffickers have learned how to leverage newer air parcel distribution methods that vary from the traditional brick-and-mortar retail model (for example, imports arriving via large cargo containers with domestic distribution networks). This is an issue that must be directly addressed by firm actions from CBP.

Section 321 De Minimis Exemption and Counterfeit Trafficking

Under Section 321 of the Tariff Act of 1930, as amended by the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA), articles with a value of $800 or less, imported by one person on one day, can be admitted free of duty and taxes. Under 19 CFR § 10.151 and 19 CFR part 143, Subpart C, those importations are often not subject to the same formal customs procedures and rigorous data requirements as higher-value packages entering the United States. Instead, the low-value shipments can be admitted into U.S. commerce with the presentation of a bill of lading or a manifest listing each bill of lading and a limited data set. The relatively limited nature of the data requirements complicates the identification of high-risk goods by CBP and other enforcement agencies. Under 19 CFR § 143.22, CBP has existing authority to require formal entry (and the complete data set for any shipment) for any merchandise, if deemed necessary for import admissibility enforcement purposes; revenue protection; or the efficient conduct of customs business.

Warehouses, Fulfillment Centers and Counterfeit Trafficking

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 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.

6. Private Sector Outreach and Public Comment

This report benefitted from extensive outreach to, and comments from, numerous private sector stakeholders in response to the FRN 2019-14715 issued on July 10, 2019. Respondents included: e-commerce platforms that operate third-party marketplaces, third-party sellers, shippers, third-party logistics providers, payment processors, and intellectual property rights holders.

Rights holders and Stakeholders Feedback

In providing comments on platforms' current preventative efforts, rights holders argued that some platforms do not do enough to ensure that sellers provide accurate information. They also stressed that the onboarding and vetting of sellers remains a concern of the highest priority.

Some commenters further argued that sellers will not be sufficiently deterred unless they can be identified and punished for promoting counterfeit and pirated goods via online platforms. Further, they contended that platforms should be more proactive in their approach to combating IPR theft and misuse. Commenters also advised that the lack of relevant policies and procedures to verify sellers' true names and addresses, and to conduct the necessary vetting and due diligence, contributes to a range of impediments to effective enforcement.

Rights holders widely view the present legislative landscape for online enforcement — where online intermediaries are generally not strictly liable for the products sold on their marketplaces by third parties — to be out of date. While in the brick-and-mortar economy, contributory infringement liability has been well-developed through case law for the licensing and oversight of

sellers, a comparable regime is largely non-existent in the e-commerce realm. A key problem here is that the laws that apply today have remained largely unchanged since the early days of e-commerce. They were developed at a time when Congress' primary concern was to avoid over-regulation of the nascent market — as exemplified by the numerous safe harbors and limitations on liability for third-party intermediaries.

Rights holders further argued that the current rules, regulations, and practices governing e-commerce disproportionately place the burden of enforcement on rights holders. While e-commerce platforms that operate third-party marketplaces provide various tools for rights holders to report counterfeit listings of their brands, they have effectively shifted the primary responsibility to monitor, detect, and remove infringing products to the rights holders.

Commenters also noted several disparities across e-commerce platforms. For example, among third-party marketplaces that control who may list products on their site for sale, some scrutinize their sellers much more than others. Some allow anyone to sell a product if they provide basic information about themselves, such as credit card and tax identity information. Others require more detailed information, such as an existing online presence, proof that the seller is a business entity and not an individual, and that the seller has established customer support.

Submissions were also received from several platforms noting that they have invested heavily in proactive efforts to prevent counterfeits from reaching their online stores, and several commenters noted that some platforms have significant interactions with law enforcement to combat counterfeits trafficking. Additionally, there was concern expressed by some respondents that while several of the leading online platforms have built out substantial programs, mandating that these practices be adopted by all online platforms could have significant consequences for smaller competitors.

Observations in Support of Strong Government Action

Five observations emerged from this stakeholder outreach and a broader review of the e-commerce landscape: first, actions by the private sector components of the e-commerce supply, distribution, and sales chain will be critical to reducing the heavy volume of counterfeit and pirated goods circulating in the U.S. economy. This is particularly true for third-party marketplaces, which provide tools that producers of counterfeit and pirated goods can exploit.

With respect to such actions, platforms are increasingly developing methods to remove counterfeit listings and compensate consumers who have unwittingly purchased counterfeit goods. Platforms are also improving their capabilities to more quickly identify counterfeits as well as identify product sectors that are more vulnerable to counterfeiting.

Second, despite such actions, private stakeholders have fallen far short of adequately addressing the substantial challenges that must be surmounted if the trafficking of counterfeit and pirated goods is to be deterred. Such trafficking continues to grow both in the volume and array of goods trafficked. A key failing within the private sector is a lack of a commonly accepted set of best practices to combat counterfeit trafficking.

Third, rights holders are often burdened by e-commerce platforms that operate third-party marketplaces with a disproportionate share of the costs of monitoring, detection, and enforcement falling on rights holders. This burden falls heavily on smaller American enterprises that cannot spread the costs due to trademark infringements and brand enforcement over large sales and inventories.

Fourth, no amount of officers or government resources alone can stem this trafficking.

Fifth, absent the adoption of a set of best practices and a fundamental realignment of incentives brought about by strong government actions, the private sector will continue to fall far short in policing itself. Indeed, the current incentive structure tends to reward the trafficking in counterfeit and pirated goods more than these incentives help to deter such trafficking.

The next two sections of this report identify a set of strong government actions that DHS, in consultation with the interagency, believes is necessary to bring about this fundamental realignment of incentives — and thereby ensure that e-commerce stakeholders appropriately shoulder much more of the responsibility for preventing the online trafficking in counterfeit and pirated goods.

7. Immediate Action by DHS and Recommendations for the USG

CBP and ICE are the primary federal agencies responsible for securing America's borders. A key responsibility is to prevent goods that infringe U.S. copyrights, registered trademarks, and certain patents from entering the United States. CBP's interdiction of counterfeit goods at U.S. Ports of Entry (POE) is the frontline of USG IPR enforcement.

In meeting their responsibilities, CBP and ICE have the statutory authority to inspect *any* package as it is imported into U.S. territory. CBP and ICE may draw upon numerous other authorities to stop and prevent the trafficking of counterfeit and pirated goods, from the assessment of civil fines and other penalties to debarring and suspending irresponsible actors. Many of these authorities are underutilized or underdeveloped to match the risks in the evolving e-commerce environment.

The previous sections of this report have provided an overview of the counterfeit trafficking landscape and identified key problems that need to be addressed firmly and swiftly. This section identifies a set of actions DHS will make through enforcement actions, sub-regulatory changes, and as necessary, notice and comment rulemaking or requested statutory amendments. These actions are summarized in the following table:

Immediate Actions to be Taken by DHS and Recommendations for the U.S. Government
1. Ensure Entities with Financial Interests in Imports Bear Responsibility
2. Increase Scrutiny of Section 321 Environment
3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Posts
4. Apply Civil Fines, Penalties and Injunctive Actions for Violative Imported Products

5. Leverage Advance Electronic Data for Mail Mode
6. Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION) Plan
7. Analyze Enforcement Resources
8. Create Modernized E-Commerce Enforcement Framework
9. Assess Contributory Trademark Infringement Liability for Platforms
10. Re-Examine the Legal Framework Surrounding Non-Resident Importers
11. Establish a National Consumer Awareness Campaign

Unless the trafficking of counterfeit and pirated goods is greatly reduced, Americans will continue to face unacceptably high health and safety risks, American enterprises and workers will continue to endure severe negative impacts, innovation and economic growth will suffer, and America will continue to be exposed to significant national security risks.

1. Ensure Entities with Financial Interests in Imports Bear Responsibility

DHS will pursue a modernized enforcement and regulatory framework that reflects the economic realities of international e-commerce and ensures that the flow of contraband is stopped at its source.

- CBP will adjust its entry processes and requirements, as necessary, to ensure that all appropriate parties to import transactions are held responsible for exercising a duty of reasonable care.

- CBP will treat domestic warehouses and fulfillment centers as the ultimate consignee for any good that has not been sold to a specific consumer at the time of its importation. As discussed in this report, counterfeit products evade detection and sit in fulfillment centers waiting for purchase by a consumer. By treating domestic warehouses and fulfillment centers as consignees in such circumstances, CBP can enhance their ability to identify Section 321 abuses consistent with current authorities, as well as use its other statutory and regulatory authorities to combat trafficking of counterfeit goods in the possession of domestic warehouses and fulfillment centers.

- DHS will encourage platforms and other third-party intermediaries that own or operate warehouses or fulfillment centers to pursue, in coordination with rights holders, bulk abandonment and destruction of contraband goods that were not interdicted by CBP but are in the platform's or other third-party intermediary's possession in a warehouse or fulfillment center. In cases where CBP suspects merchandise destined for a U.S. fulfillment center violates trade laws prohibiting importation of counterfeit goods and initiates a seizure process for merchandise, CBP will notify the platform or other third-party intermediary operating the fulfillment center or warehouse and request they pursue abandonment and destruction with the rights holders of any identical offending goods in their possession. Failure to cooperate following such notification could be a factor when CBP and ICE identify counterfeit cases to pursue under their existing authorities.

- CBP will require formal entry for shipments deemed high-risk, notwithstanding that such shipments might otherwise qualify for duty-free or informal entry treatment. High-risk merchandise shall include those categories of goods that pose an elevated risk of counterfeiting and shall consider the source of the merchandise.

- CBP will address such high-risk shipments within its current bonding regime, developing a framework for a new type of bond specifically for counterfeit risk (like bonds required for anti-dumping and countervailing duties).

- In consultation with the Department of Justice, CBP will provide guidance regarding the types of customs violations that could be actionable under the False Claims Act (FCA) and will make information regarding successful FCA claims publicly available to inform and enable the public to identify and bring such violations to the attention of the government.

2. Increase Scrutiny of Section 321 Environment

As described above, existing laws and administrative practices may not sufficiently define responsibilities in the e-commerce environment, including who within an e-commerce transaction bears responsibility and legal liability for illicit merchandise and other violations. Statutes and administrative practices can be clarified and updated to provide greater transparency and information about the various parties involved so that DHS can identify high-risk transactions, interdict dangerous merchandise, and cause bad actors to pay the price for their actions. To address this problem in the Section 321 environment, CBP shall require data that sufficiently identifies the third-party seller and the nature and value of the imported merchandise, as well as other information that is necessary to determine the responsible party for Section 321 eligibility purposes, consistent with existing legal authorities. This will be informed by the following efforts:

- **Gather Information through Pilot Program.** CBP has been examining different e-commerce platform business models and has initiated several pilot programs designed to better understand the dynamics involved, and the type of information that the government should be collecting, including the "Section 321 Data Pilot" specifically for Section 321 entries, 84 Fed Reg. 35405 (July 23, 2019). CBP plans to continue these efforts for approximately two years and will use the information gained to better target counterfeits in the Section 321 environment, to help shape the scope of further policy formation, and ensure compliance with customs laws.

- **Enhanced Data Requirements.** Upon collection of adequate amounts of data through the Section 321 Data Pilot to identify gaps in the current data collection framework, but no later than six months from the issuance of this report, CBP will, consistent with applicable law, take all necessary steps — including, as applicable, issuing a notice of proposed rulemaking — to initiate a new data collection process. This process will include collecting certain information from domestic warehouses or fulfillment centers about third-party sellers in transactions for which the third-party seller utilizes a domestic warehouse or fulfillment center to store inventory for further sale to domestic consumers. The collection will also include data that sufficiently identifies the third-party seller and the nature and

value of the imported merchandise, as well as other information that is necessary to determine the responsible party for Section 321 eligibility purposes, consistent with existing legal authorities. As appropriate, the domestic warehouse or fulfillment center may be deemed the "person" for Section 321 eligibility if the warehouse or fulfillment center fails to provide CBP with such information.

- **Issue Guidance.** To prevent abuse of Section 321, CBP will develop administrative guidance and, if necessary, consider whether promulgating new regulations is necessary to better define and subsequently enforce Section 321 eligibility requirements. At a minimum this guidance will address the following:

    - What value needs to be reported for a Section 321 entry; and

    - What information will be necessary to uniquely identify the ultimate consignee.

3. Suspend and Debar Repeat Offenders; Act Against Non-Compliant International Postal Operators

In appropriate circumstances, CBP and ICE currently take steps to add persons (both entities and individuals) that have been found to lack present responsibility to the federal suspension and debarment list. Those persons on this suspension and debarment list are prohibited from participating in both government procurement and certain other non-procurement activities. However, current agency practices continue to permit these persons to obtain importer of record numbers and import goods into the United States.

Explicitly clarifying the scope of suspension and debarment to prevent participation in the importer of record program by amending Executive Order 12549 will assist CBP in requiring regulated entities to screen their customers against the suspension and debarment list. This will improve targeting and reduce the number of packages sent by repeat offenders, thereby stopping the flow of contraband at their sources.

- CBP recommends amending Executive Order 12549 to explicitly bar suspended and debarred persons from participating in the Importer of Record Program.

- Following such an amendment, or as otherwise consistent with applicable law and Executive Orders, CBP will require express consignment operators, carriers, and hub facilities to verify their customers have not been suspended or debarred from participating in the Importer of Record Program and refuse to provide import-related services to such suspended or debarred customers.

- Consistent with applicable law, CBP will condition continued access to its "trusted trader programs" by express consignment operators, carriers, and hub facilities on compliance with this verification process that determines whether a customer has been suspended or debarred.

- Consistent with applicable law, CBP also will identify non-compliant international postal operators and international posts by developing an International Mail Non-Compliance metric and will take enforcement actions based on these metrics.

4. Apply Civil Fines, Penalties, and Injunctive Actions for Violative Imported Products

It is critical to the integrity of e-commerce and for the protection of consumers and rights holders that e-commerce platforms that operate third-party marketplaces, and other third-party intermediaries assume greater responsibility, and therefore greater liability for their roles in the trafficking of counterfeit and pirated goods. To that end, CBP and ICE will use existing statutory and regulatory authorities to reach the activities of third-party marketplaces and other intermediaries where evidence demonstrates they have unlawfully assisted in the importation of counterfeit and pirated goods through the following actions:

- CBP and ICE will immediately begin to identify cases in which third-party intermediaries have demonstrably directed, assisted financially, or aided and abetted the importation of counterfeit merchandise. In coordination with the Department of Justice, CBP and ICE will seek all available statutory authorities to pursue civil fines and other penalties against these entities, including remedies under 19 U.S.C. § 1526(f), as appropriate.

- DHS recommends the administration pursue a statutory change to explicitly permit the government to seek injunctive relief against third-party marketplaces and other intermediaries dealing in counterfeit merchandise.

- In the interim, DHS will provide information and support to registered brand owners looking to utilize statutory authorities to seek injunctive relief against persons dealing in counterfeit merchandise, whether through direct sales or facilitation of sales, following seizures of goods that are imported contrary to law.

- ICE shall prioritize investigations into intellectual property-based crimes regardless of size and will make referrals for all such investigations where appropriate.

- ICE will coordinate with the Department of Justice to develop a strategy to investigate and prosecute intellectual property violations at all levels of the supply chain at a sufficiently high level to respond to the concerns raised in this report and according to its budget and broader mission goals.

5. Leverage Advance Electronic Data for Mail Mode

The United States Postal Service (USPS) is responsible for the presentation of mail and the provision of advance electronic data (AED) to CBP for arriving international mail parcels. USPS receives such AED from international posts. As has been noted, given the number of e-commerce transactions that are sent by mail, there is a significant gap in the information CBP receives. USPS and CBP have enhanced their collaboration in the targeting and identification of offending

merchandise that is imported through international mail. Both agencies are implementing new strategies for leveraging the AED already available to identify offending merchandise by taking the following actions:

- DHS and USPS have signed a letter of intent that enables the USPS to work alongside CBP during special operations to become a force multiplier in the interdiction of counterfeit products.

- Upon completion and publication of the Synthetics Trafficking and Overdose Prevention (STOP) Act implementing regulations, DHS will use information gleaned from the 321 Data Pilot and will make recommendations to USPS to address any critical data gaps that remain between what is required of mail versus air cargo. At a minimum, this effort will seek to enhance the individualized tracking of international mail parcels sent through air cargo.

6. Plan for ACTION

Counterfeit networks can be complex and multidimensional, exploiting legal and regulatory nuances in the different stages and aspects of international trade. Yet, for a variety of reasons, including competition law and trade secrets protection, various stakeholders in the e-commerce supply and distribution chains historically have not shared information on problematic sellers, shippers, freight forwarders, brokers, and other third-party intermediaries involved in counterfeit trafficking.

To address this issue, the IPR Center established the E-Commerce Working Group (ECWG) to foster and encourage the flow of actionable data and information between platforms and relevant third-party intermediaries as well as affected carriers, shippers, search engines, and payment processors. DHS supports the efforts of the IPR Center's ECWG and recommends the formation of the Anti-Counterfeiting Consortium to Identify Online Nefarious Actors (ACTION). Specific ACTION efforts will include the following:

- Sharing information within the ACTION framework on sellers, shippers, and other third-party intermediaries involved in trafficking in counterfeit and pirated goods.

- Sharing of risk automation techniques allowing ACTION members to create and improve on proactive targeting systems that automatically monitor online platform sellers for counterfeits and pirated goods.

- In addition, ACTION members may enter non-binding memoranda of understanding (MOU) with the IPR Center, consistent with U.S. law, to clarify the expectations and legal understanding for data sharing and coordinated IPR enforcement moving forward. Such MOUs will provide a vehicle to create a compliance scoring mechanism, as well as to delineate reasonable efforts to know the seller as well as the scope of products involved

(e.g., fast-moving consumer goods, consumer electronics, fashion and luxury products, sports goods, software, and games, and toys).

7. Analyze Enforcement Resources

Packages shipped through the international mail environment account for approximately 500 million packages annually. This does not include the millions of packages sent out daily via express consignment carriers. Amidst this flood of packages, insufficient resources can create a key limitation on the capabilities of DHS and other government agencies to screen, target, and detect the counterfeit and pirated goods that hide amongst the increasing massive flow of small packages.

A lack of resources also limits the ability of intelligence gathering and analysis, the proper determination of whether suspect goods may be counterfeit, the collection of comprehensive data on the trafficking in counterfeit and pirated goods, and the ability to conduct criminal investigations into the organizations that traffic in counterfeit goods. To address these issues, the following actions shall be taken:

- CBP will analyze whether the fees collected by CBP are currently set at sufficient levels to reimburse the costs associated with processing, inspecting, and collecting duties, taxes, and fees for parcels. CBP shall also provide recommendations to the Department of the Treasury regarding any fee adjustments that would be necessary to fund and reimburse the federal government's costs for more effectively combating the trafficking of counterfeit and pirated goods.

8. Create Modernized E-Commerce Enforcement Framework

DHS will pursue a modernized enforcement framework that reflects the economic realities of international e-commerce. This new framework may rely on the provision of privileges or benefits by CBP to e-commerce entities in exchange for the submission of additional data elements and sufficient internal controls that demonstrate the entities' ability to identify and manage risk within their respective supply chains. This new framework may also require updates to existing statutes and regulations to underpin this effort. Key elements of a modernized e-commerce enforcement framework could include, but are not limited to:

- Seeking statutory authority to treat IPR infringing goods as summarily forfeited upon discovery by CBP or ICE similar to the treatment of Schedule I and II narcotics under Title 21 of the U.S. Code. This will send a clear message about the importance of IPR enforcement, and simultaneously streamline the disposition of CBP enforcement actions.

- Pursuing statutory and/or regulatory changes, as necessary, so that CBP can better share information with the private sector;

- Implementing a risk-based bonding regime for e-commerce transactions; and

- Adopting streamlined enforcement processes for seized, abandoned, and forfeited goods.

9. Assess Contributory Trademark Infringement Liability for E-Commerce

Online platforms have avoided civil liability for contributory trademark infringement in several cases. Given the advance and expansion of e-commerce, DHS recommends that the Department of Commerce consider the following measures:

- Assess the state of liability for trademark infringement considering recent judicial opinions, and the impact of this report—including platforms' implementation of the best practices directed herein.

- Seek input from the private sector and other stakeholders as to the application of the traditional doctrines of trademark infringement to the e-commerce setting, including whether to pursue changes in the application of the contributory and/or vicarious infringement standards to platforms.

10. Re-Examine the Legal Framework Surrounding Non-Resident Importers

Currently, non-resident importers can legally enter goods into the United States provided they have a "resident agent" as defined in regulation. In practice, it can be difficult to compel non-resident importers to pay civil penalties and respond to other enforcement actions available to the USG. With this in mind, DHS should reevaluate the legal framework for allowing non-resident importers in the Section 321 *de minimis* low-value shipment environment.

11. Establish a National Consumer Awareness Campaign

Given the critical role that consumers can play in the battle against online counterfeiting, DHS recommends the development of a national public-private awareness campaign. The national public awareness campaign recommended by DHS should involve platforms, rights holders, and the applicable government agencies to provide education for consumers regarding the risks of counterfeits as well as the various ways consumers can use to spot counterfeit products. At present, many consumers remain uninformed as to the risks of buying counterfeit and pirated products online. These risks are both direct to them (e.g., tainted baby food), as well as indirect (e.g., sales revenues can fund terrorism).

Many consumers are also unaware of the significant probabilities they face of being defrauded by counterfeiters when they shop on e-commerce platforms. As this report has documented, these probabilities are unacceptably high and appear to be rising. Even those consumers motivated to conduct research and stay informed might lack the specialized knowledge and efficient user tools to make diligent online buying decisions.

A strong and ongoing national campaign to increase public awareness about the risks of counterfeits in an e-commerce world should help alert consumers about the potential dangers of some online purchases. To the extent e-commerce platforms empower their consumers to participate in the monitoring and detection of counterfeits, e.g., by implementing several of the best practices recommended in this report, this will also help in the fight against the trafficking in counterfeit and pirated goods.

This effort could use technology as well as provide online education. For example, online marketplaces could prominently display messages on their home pages, as well as on high-risk item pages, warning customers about the dangers of counterfeits and urging respect for intellectual property rights. Additionally, the campaign could be paired with technologically-enabled assurances of authenticity. Such an approach would provide commercial advantages to the platforms that adopt it while also benefiting consumers and rights holders through reliable methods to identify and certify the authenticity of branded products across online platforms.

8. Private Sector Best Practices

The following table catalogs a set of high priority "best practices" that should be swiftly adopted by e-commerce platforms that operate third-party marketplaces, and other third-party intermediaries. Under the authority of the Secretary of the Department of Homeland Security, these best practices shall be recommended and communicated to all relevant private sector stakeholders by the ICE/HSI-led IPR Center.

It shall be a duty of the IPR Center to encourage, monitor, and report on the adoption of, and the progress and effectiveness of, these best practices, through all means necessary within the scope of the legal authority of DHS and the Federal Government.

Best Practices for E-Commerce Platforms and Third-Party Marketplaces
1. Comprehensive "Terms of Service" Agreements
2. Significantly Enhanced Vetting of Third-Party Sellers
3. Limitations on High Risk Products
4. Efficient Notice and Takedown Procedures
5. Enhanced Post-Discovery Actions
6. Indemnity Requirements for Foreign Sellers
7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests
8. Pre-Sale Identification of Third-Party Sellers
9. Establish Marketplace Seller IDs
10. Clearly Identifiable Country of Origin Disclosures

1. Comprehensive "Terms of Service" Agreements

It is critical that platforms require all third-party sellers to sign comprehensive and stringent terms of service agreements that maximize the authorities of the platforms to combat counterfeit

trafficking. Terms of service agreements will provide platforms with an important legal means to combat counterfeit trafficking

Most obviously, these terms of service should incorporate explicit prohibitions on selling counterfeit and pirated goods. Once the platform has affirmatively detected infringement on a seller profile, the actions listed below under the category of "post-discovery actions" should be allowed under the terms and taken swiftly.

The terms of service should also list the potential repercussions sellers face for violations. Generally, these repercussions should allow platforms to impose sanctions such as suspension, termination, and debarment without waiting for a determination by a court for sellers who violate the terms of the agreement. The terms should include escalating capabilities to suspend, terminate, and debar counterfeit traffickers and their affiliates.

Specifically, they should allow the platform to conduct, at a minimum, the following actions in response to violations or identified risk factors in the seller's profile and product postings without waiting for a determination by a court:

> (1) terminate or suspend a seller account based on the use or reference to a username that is confusingly similar to a registered trademark;
>
> (2) take down or suspend and keep down individual product postings based on the misuse of photographs, logos, external links to infringing content, certain coded messages with actual intellectual property references removed, or imbedded offers to manufacture; and
>
> (3) allow for an escalating enforcement structure that results in (for major infractions and/or repeat minor infractions) permanent removal of the seller, and any known related seller profiles, from the marketplace feature of the platform and further results in forfeiture and destruction of all offending goods in warehouses or fulfillment centers operated by, or under the control of, the platform.

To maximize platform authorities, and as explained further below, such terms of service should also allow platforms to impose appropriate limitations on products listed, require clearly identifiable country of origin disclosures, impose U.S. banking and indemnity requirements, and significantly improve pre-sale identification of third-party sellers.

2. Significantly Enhanced Vetting of Third-Party Sellers

Significantly enhanced vetting of third-party sellers is one of the most effective forms of due diligence platforms can engage in to reduce the risk of counterfeits entering the e-commerce stream. Platforms should have a uniform and articulable vetting regime to determine if a seller will be allowed to list products for sale.

To facilitate enhanced vetting, platforms should, at a minimum, require 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

(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).

Information provided by potential sellers should also be vetted for accuracy, including through the following efforts:

(1) use of technological tools, as well as analyses of historical and public data, to assess risk of sellers and products; and

(2) establishment of an audit program for sellers, concentrating on repeat offenders and those sellers exhibiting higher risk characteristics.

Any failure to provide accurate and responsive information should result in a determination to decline the seller account and/or to hold the seller in violation of the platform's terms of service.

3. Limitations on High Risk Products

Platforms should have in place protocols and procedures to place limitations on the sale of products that have a higher risk of being counterfeited or pirated and/or pose a higher risk to the public health and safety. For example, some of the major platforms completely prohibit the sale of prescription medications by third-party sellers in their marketplaces. Many platforms also ban the sale of products that are known to be particularly vulnerable to counterfeiting and that pose a safety risk when sold online. Examples include car airbag components, infant formula, and new batteries for cellular phones.

Platforms can also place other types of restrictions on third-party sellers before certain high-risk categories of goods may be sold. For example, some platforms require prior approval for items such as automotive parts, jewelry, art, food, computers, sports collectibles, DVDs, and watches that are particularly prone to counterfeiting.

Platforms should prominently publish a list of items that may not be sold on third-party marketplaces under any circumstances (prohibited), as well as a list of items that can only be sold when accompanied by independent third-party certification (restricted). In constructing these lists, platforms should consider, among other things, whether a counterfeit version of the underlying product presents increased risks to the health and safety of U.S. residents or the national security of the United States. When a seller claims their merchandise has an independent third-party certification, and this certification is required in order for the product to be legally offered for sale

in the United States, platforms should make good-faith efforts to verify the authenticity of these certifications.

4. Efficient Notice and Takedown Procedures

Notice and takedown is the most common method of removing counterfeit listings from third-party marketplaces and e-commerce platforms. This noticing process can be particularly time-consuming and resource-intensive for rights holders who currently bear a highly disproportionate share of the burden of identifying the counterfeit listings for noticing.

These rights holders must invest significant resources to scour millions of listings across multiple platforms to identify potentially counterfeit listings and notify the third-party marketplace or e-commerce platform. This kind of comprehensive policing of e-commerce often is not possible for smaller enterprises.

As a further burden, some third-party marketplaces require rights holders to buy the suspected products from the sellers to verify that they are in fact counterfeit. There often is a delay of a day or longer between the time that notice is provided, and the time listing is removed. During this period, counterfeiters may continue to defraud American consumers.

To address these abuses — and assume a much greater share of responsibility for the policing of e-commerce — platforms should create and maintain clear, precise, and objective criteria that allow for quick and efficient notice and takedowns of infringing seller profiles and product listings. An effective regime should include, at a minimum, the following: (1) minimal registration requirements for an interested party to participate in the notice and takedown process; (2) reasonable rules that treat profile owners offering large quantities of goods on consumer-to-consumer platforms as businesses; and (3) transparency to the rights holders as to how complaints are resolved along with relevant information on other sales activity by the seller that has been implicated.

5. Enhanced Post-Discovery Actions

Upon discovery that counterfeit or pirated goods have been sold, platforms should conduct a series of "post-discovery" actions to remediate the fraud. These should include:

(1) notification to any buyer(s) likely to have purchased the goods in question with the offer of a full refund;

(2) notification to implicated rights holders, with details of the infringing goods, and information as to any remaining stock of the counterfeit and pirated goods held in warehouses;

(3) implementation of practices that result in the removal of counterfeit and pirated goods within the platform's effective control and in a manner that prevents such goods from re-entering the U.S. or being diverted to other markets; and

(4) immediate engagement with law enforcement to provide intelligence and to determine further courses of action.

6. Indemnification Requirements for Foreign Sellers

For a large portion of e-commerce, foreign sellers do not provide security or protection against a loss or other financial burden associated with the products they sell in the United States. Because these sellers are located outside the United States, they also may not be subject to the jurisdiction of U.S. courts in civil litigation or government enforcement actions. Further adding to this liability gap, there is this: while e-commerce platforms generally have a U.S. presence and are under U.S. jurisdiction, under the current interpretations of American laws and regulations, they are often found not to be liable for harm caused by the products they sell or distribute.

The result of this jurisdictional and liability gap is that consumers and rights holders do not have an efficient or predictable form of legal recourse when they are harmed by foreign products sold on third-party marketplaces. Accordingly, e-commerce platforms should require foreign sellers to provide some form of security in cases where a foreign product is sold to a U.S. consumer. Such form of security should be specifically designed to cover the potential types and scope of harm to consumers and rights holders from counterfeit or pirated products.

Note that there are several ways that platforms might flexibly achieve this goal. For example, requiring proof of insurance would provide a form of security for any reasonably foreseeable damages to consumers that might flow from the use of the product. Rights holders could also be compensated in cases of infringement.

7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests

Many foreign sellers on third-party marketplaces do not have a financial nexus to the United States, making it difficult to obtain financial information and to subject all parts of the transaction to U.S. law enforcement efforts.

Platforms should close this loophole by encouraging all sellers to clear transactions only with banks and payment providers that comply with U.S. law enforcement requests for information and laws related to (relevant to) the financing of counterfeit activity.

8. Pre-Sale Identification of Third-Party Sellers

Stakeholders have, at times, reported that buyers have been surprised to discover upon completion of an online sales transaction, that the order will be fulfilled by an unknown third-party seller and *not* the platform itself. Without addressing the separate legal question of whether this comprises deceptive action *per se*, at least some buyers may have made different purchasing decisions if they

had known, prior to purchase, the identity of the third-party "storefront" owner, and/or the party ultimately responsible for fulfilling the transaction.

To increase transparency on this issue, platforms should significantly improve their pre-sale identification of third-party sellers so that buyers can make informed decisions, potentially factoring in the likelihood of being sold a counterfeit or IPR infringing merchandise. Platforms should implement additional measures to inform consumers, prior to the completion of a transaction, of the identity of storefront owners and/or those responsible for fulfilling a transaction, as well as any allegations of counterfeits being sold by a particular seller. On the converse, if a particular seller is a licensed reseller of the product, this information should also be provided.

Even if this information may be currently available, firm steps should be taken to ensure that this information is featured prominently in product listings. This will prompt greater consumer awareness and lead to more informed decision-making.

9. Establish Marketplace Seller IDs

Platforms generally do not require a seller on a third-party marketplace to identify the underlying business entity, nor to link one seller profile to other profiles owned by that same business, or by related businesses and owners. In addition, the party that appears as the seller on the invoice and the business or profile that appears on the platform to be the seller, may not always be the same. This lack of transparency allows one business to have many different profiles that can appear unrelated. It also allows a business to create and dissolve profiles with greater ease, which can obfuscate the main mechanism that consumers use to judge seller credibility, namely reviews by other buyers.

Platforms should require sellers to provide the names of their underlying business or businesses (if applicable), as well as any other related seller profiles owned or controlled by that seller or that clear transactions through the same merchant account. Platforms can use this seller ID information in three helpful ways:

First, to communicate to the consumer a more holistic view of "who" is selling the goods, allowing the consumer to inspect, and consult reviews of, all related seller profiles to determine trustworthiness. Second, linking all related sellers together will assist rights holders in monitoring who is selling goods that they believe to be infringing. Third, the platform can use the connections to other seller profiles to better conduct its own internal risk assessment, and make risk mitigation decisions (e.g., requiring cash deposits or insurance) as appropriate based on the volume and sophistication of the seller.

10. Clearly Identifiable Country of Origin Disclosures

Brick-and-mortar retail stores are required to have labels on their products that clearly identify the country or countries of origin. No such requirement applies to online e-commerce.

Platforms should require sellers to disclose the country of origin of their products; and platforms should post this country of origin information for all the products they sell. This will assist both the platforms and consumers in evaluating the risks that a product might be counterfeit.

9. Conclusions

Both private sector and USG input to this report have shown that the flood of counterfeit and pirated goods now being trafficked to American consumers through online third-party marketplaces is threatening both the public health and safety as well as national security. The lack of effective methods for addressing counterfeit goods stifles American innovation and erodes the competitiveness of U.S. manufacturers and workers. Despite increased efforts of both the USG and private sector stakeholders, the trafficking of counterfeit and pirated goods continues to worsen, in both the volume and the array of products being trafficked.

This report to President Donald J. Trump has identified a set of strong government actions that DHS and other federal agencies can begin executing immediately to address a crisis that is undermining America's trust in e-commerce even as it is exposing the American public to undue and unacceptable risks.

Additionally, this report has proposed a set of best practices for private sector stakeholders that DHS believes should be adopted swiftly. As the longstanding experiences of brick-and-mortar stores demonstrate, the private sector is capable of operating businesses that sell legitimate, not illicit, goods to American consumers. We should expect the same level of care from online third-party marketplaces that we expect from the stores physically located in our communities.

During the time you have spent reading this report, hundreds of thousands of new clicks in online third-party marketplaces have started the process for a new wave of counterfeits flooding into the United States. Although the USG will continue to benefit from additional information flowing from current-running pilot programs, and longer-term legislative and regulatory efforts, the time has come for action, both from the USG and those private sector companies that desire to be good partners in combating the scourge of counterfeiting.

10. Appendix A: The IPR Center

The National Intellectual Property Rights Coordination Center (IPR Center) is led by Homeland Security Investigations. The IPR Center plays an important role in consumer and rights holders education on the dangers of purchasing counterfeit goods and on how to report a suspected counterfeit to law enforcement.

In 2018, the IPR Center conducted 192 IPR and commercial fraud-related outreach efforts, reaching 12,061 people. As recommended in this report, this IPR Center should play a critical and expanded role in the ongoing battle against counterfeit trafficking.

This Appendix describes some of the major initiatives the IPR Center is currently involved in.

Background on the IPR Center

The IPR Center brings together 25 U.S Government and foreign government agencies in a task force setting using a three-pronged approach to combat intellectual property and trade crime: interdiction, investigation, and outreach to the public and law enforcement. It seeks to coordinate a unified USG response to the growing threat of counterfeiting and has significantly expanded the original multi-agency law enforcement and regulatory endeavor created to target IPR crimes.

As part of this effort, rights holders, online marketplaces, payment processers and companies involved in all points across the supply chain regularly meet with members of the IPR Center to share their best practices, concerns, and suggestions. The information gathered at these events can lead to further collaboration across sectors to develop innovative solutions to complex cross-cutting challenges, including enhanced information sharing, joint enforcement actions, and specialized, targeted training and outreach.

IPR Training

The IPR Center, with assistance from the Department of State, works closely with International Narcotics and Law Enforcement Affairs (DOS/INL) and DOJ International Computer Hacking and Intellectual Property Section (formerly Intellectual Property Law Enforcement Coordinator - IPLEC). In conjunction with ICE Attaché offices, the IPR Center directs, organizes and delivers regional IPR training in the form of lectures and presentations to foreign customs, police, prosecutors, and magistrates.

IPR Center training programs are usually 3-5 days in length and emphasize IPR enforcement, particularly the investigation and prosecution of IPR violations and associated crimes such as smuggling and money laundering.

The training programs are interactive workshops led by subject matter experts and focus on health and safety risks associated with counterfeited items such as pharmaceuticals, electronics, automotive parts, and health and beauty products. With the growing number of e-commerce marketplaces, the training programs have an Internet-investigations focus as well.

Private sector representatives or associations are also invited to participate in the training programs to highlight the challenges their industry sector may face in a particular region and to highlight the necessity of government and industry cooperation.

Automotive Anti-Counterfeiting Council

The IPR Center meets regularly with automotive original equipment manufacturers through the Automotive Anti-Counterfeiting Council (A2C2) to address the sale and distribution of counterfeit parts and components to unsuspecting consumers, including the distribution of counterfeit parts through third-party marketplaces. The IPR Center and the A2C2 work together to provide training to federal and local law enforcement partners and payment processors on recognizing counterfeit automotive parts and conducting criminal investigations and prosecutions.

Defense Industrial Base Supply Chain

Addressing counterfeits in the defense industrial base supply chain is critical to national security. A faulty counterfeit product can harm not only the individual who uses it. It can impact the safety and security of the entire country if dangerous counterfeits are used in combat situations.

The Defense Federal Acquisition Regulation Supplement (DFARS) is a Department of Defense (DOD)-specific supplement to the Federal Acquisitions Regulation (FAR), which establishes government-wide regulations governing executive agency procurement contracts. DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, requires that certain government contractors institute and implement a counterfeit detection and avoidance system for electronic parts, including establishing the minimum requirements for such a system and penalties for a failure to comply. In addition, contractors can recover the costs of any rework or corrective action taken to remedy any counterfeits parts from subcontractors.

Operation Chain Reaction (OCR) is an ICE-led initiative at the IPR Center that targets counterfeits entering the supply chains of the DOD and other USG agencies. OCR began in June 2011, and it combines the expertise of 17 federal agencies. Each year, the OCR Task Force co-hosts the Counterfeit Microelectronics Working Group (CMWG) with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS). Attendees include representatives from industry, law enforcement, Department of Defense (DOD), and Assistant United States Attorneys (AUSAs). The focus of the meetings is to enhance communication between law enforcement and industry and discuss the latest trends in the counterfeiting of integrated circuits. The CMWG's role is to protect the DOD supply chain through extensive collaboration.

11. Appendix B: Ongoing CBP Activities to Combat Counterfeit Trafficking

This appendix provides a brief summary of some of the major activities CBP and DHS engage in as part of the battle against the trafficking of counterfeit and pirated goods.

National Targeting Center

CBP's National Targeting Center (NTC) carries out daily targeting on IPR recidivists, which often use third-party marketplaces for counterfeit trafficking. It makes referrals to the IPR Center for review and distribution to its field offices for further investigation. It also provides real time IPR case support for Homeland Security Investigations and collaborates with the NTC's investigations division to collaborate on IPR criminal leads and existing cases.

COAC E-Commerce Working Group

The Commercial Customs Operations Advisory Committee (COAC) provides recommendations to the Secretaries of the Treasury and DHS on improvements to the commercial operations of CBP. The COAC consists of 20 members appointed by the Secretary of the Treasury and the Secretary of DHS.

COAC members are representative of the individuals and firms affected by the commercial operations of CBP. CBP's Office of Trade leads the COAC E-Commerce Working Group, which focuses on policy challenges surrounding the increase of e-commerce shipment volumes. The group recently finalized a supply chain map that the COAC recommended CBP use for outreach and policy-making endeavors.

Outreach

Section 311 of the Trade Facilitation and Trade Enforcement Act (TFTEA) (codified at 19 U.S.C. § 4350) calls for DHS to develop and execute an educational awareness campaign aimed at informing international travelers about the legal, economic, and public health and safety impacts of importing IPR-infringing merchandise. There have been four phases to date in the "Truth Behind Counterfeits" IPR public awareness campaign—summer 2017, holidays 2017, summer 2018, and holidays 2018.

During each of these four phases, advertisements have run on large-scale billboards in major U.S. airports throughout the country. There has also been a digital component to the campaign where the ads run on relevant travel-related websites.

CBP continues to partner with the private sector to conduct IPR risk assessments by allowing IPR owners to assist CBP in identifying authentic and low-risk shipments. CBP is also highly engaged with the private sector through participation in the IPR Working Group of the COAC's Trade Enforcement and Revenue Collection Subcommittee, and the Department of Commerce's Industry Trade Advisory Committee on Intellectual Property Rights.

In FY 2018, CBP conducted roundtables to bring together personnel from the law enforcement community and industry stakeholders for information sharing among members. This provided an opportunity for industry stakeholders to share specific industry standards with field personnel working to protect stakeholder rights at the border. In FY 2018, CBP held roundtables at the Automotive and Aerospace Center of Excellence and Expertise IPR Conference.

CBP personnel from headquarters, the ports, the centers, NTC, and the targeting groups also meet regularly with private sector stakeholders and trade associations to discuss trends, technologies, and ways to cooperate on IPR enforcement. CBP maintains IPR enforcement personnel across the country, allowing CBP personnel to meet with businesses and trade associations either at headquarters or in locations close to where the companies are located or do business. CBP personnel regularly meet with brand protection and other corporate officials on a company-specific basis.

Additionally, CBP pursues bilateral and multilateral engagements with foreign counterparts to conduct joint customs IPR enforcement operations, share effective enforcement practices, and exchange information on IPR violations to improve targeting and interdiction of counterfeit and pirated goods.

CBP, in coordination with ICE/HSI, focuses its bilateral engagement efforts on those countries with which CBP and ICE/HSI have a Customs Mutual Assistance Agreement (CMAA) and continues to pursue establishing new CMAAs with foreign governments around the world. CBP attachés stationed at embassies around the world facilitate cooperation through operational planning, information exchange, and sharing best practices between CBP and foreign customs authorities.

Training

CBP's IPR-related training focuses on training front-line and Center of Excellence and Expertise (Center) personnel on how detect, examine, and enforce IPR violations. Several offices within CBP collaborate to provide a robust IPR instructor-led training course that covers IPR seizure authority, enforcement best practices, administrative IPR procedures, and other critical legal and policy topics.

CBP's Office of Trade also conducts IPR webinars to educate port and Center personnel on IPR infringing products. Rights holders provide information on how to recognize IPR-infringing products, labels, and packaging. CBP is also developing a formalized Advanced IPR Enforcement Training course that will expand on the existing IPR Instructor-led Training course to increase students' knowledge of advanced IPR enforcement areas.

Private sector engagement also continues to comprise a significant part of CBP training for frontline personnel. Rights holders are routinely invited to address CBP audiences at local ports and the Centers. CBP also hosts national webinars with rights holders designed to train personnel across the country. Rights holders also provide CBP personnel with product identification guides

that describe methods to distinguish between genuine and infringing products. These guides afford frontline personnel the ability to compare imported merchandise with pictures of genuine products.

Additionally, CBP Regulations and Rulings provide training on advanced detection of trademark/copyright infringement to Import Specialists of the Automotive and Aerospace Center, the Consumer Products and Mass Merchandising Center, and the Apparel, Footwear and Textile Center, as well as to CBP officers at the ports of Newark, New Jersey, and John F. Kennedy Airport.

Rulemakings and Procedures

CBP has recently published two notices of proposed rulemaking related to the protection of intellectual property rights. In the first, CBP proposes to standardize the process by which customs brokers verify the identity of their clients, typically importers. The proposed regulations would formalize the verification process and require that a re-verification process be carried out by brokers every year. This improved broker knowledge is designed to allow for better commercial fraud prevention and revenue protection, and to help prevent the use of shell or shelf companies by importers who attempt to evade the customs laws of the United States. Preventing the use of shell or shelf companies by importers would help reduce the misclassification of merchandise to avoid duties, protect against IPR violations, reduce antidumping/countervailing duty infractions, and reduce the importation of unsafe merchandise.

The second proposal would create a procedure for the disclosure of information otherwise protected by the Trade Secrets Act to a trademark owner when merchandise has been voluntarily abandoned if CBP suspects that the successful importation of the merchandise would have violated U.S. trade laws prohibiting the importation of merchandise bearing counterfeit marks. This regulation will provide greater transparency for partner government agencies, as well as for rights holders; allowing both to reassess and amend their own enforcement strategies in light of contemporaneous attempts to import counterfeit and pirated goods.

Trade Special Operations

A CBP Trade Special Operation (TSO) is a comprehensive and focused trade targeting action conducted during a limited timeframe to address a specific trade enforcement risk, usually in support of one of CBP's Priority Trade Issues (PTIs), which include IPR violations. These operations target high-risk shipments at seaports, airports, CBP's international mail facilities, and express consignment carrier hubs across the United States.

Three related developments have contributed to the growth in the number of national and local TSOs and improved visibility into their results: (1) The implementation of the Automated Targeting System (ATS) Import Targeting module and the updated ATS Import Cargo module at the beginning of FY 2019; (2) the issuance of an updated TSO Standard Operating Procedures in FY 2019; and (3) the ongoing efforts of proactive trade enforcement managers collaborating within CBP's Integrated Trade Targeting Network, which meets monthly and represents all of CBP trade components (Field Offices, Centers, Headquarters, and other offices).

12. Appendix C: Homeland Security Investigations

Homeland Security Investigations (HSI) within DHS's Immigration and Customs Enforcement agency is the principal investigative arm of DHS. It is a vital U.S. asset in combating criminal organizations illegally exploiting America's travel, trade, financial and immigration systems and including the theft of intellectual property.

Investigations

HSI investigates sophisticated, complex conspiracies that span international boundaries. These investigations result in the prosecution of members of transnational criminal organizations and the seizure of illicit proceeds and contraband.

Operation In Our Sites

Since 2010, HSI has been conducting Operation In Our Sites (IOS). This operation targets criminal organizations that distribute dangerous and illicit goods via websites, online platforms, and social media sites.

Initially formed as a U.S.-based initiative for the seizure of domain name registrations, IOS has evolved to develop long term investigations that identify targets and assets in the U.S. and disrupt the financial schemes used by these organizations, both domestically and internationally.

Operation IOS has been expanded to include efforts by various European countries and coordinated by Europol (the European Union's law enforcement agency). These efforts include civil takedowns by private sector companies/groups.

In 2018, 26 countries and dozens of private sector companies participated in IOS, resulted in the criminal seizure of over 33,000 domain name registrations and the civil seizure of over 1.2 million domain name registrations.

In addition, over 2.2 million URL links to e-commerce platforms and social media platforms have been seized as a result of IOS. When a domain name registration is seized as part of IOS, Internet traffic to that site is redirected towards a seizure banner notifying visitors that the site has been seized for offering counterfeits. Since IOS began, there have been more than 177 million views of the IOS seizure banner.

On February 14, 2018, HSI also published its E-Commerce Strategic Plan. It leverages collaboration among private industry, law enforcement, and advocates for a cooperative enforcement approach to identify and dismantle organizations and prosecute people that traffic in dangerous and illicit goods utilizing various e-commerce outlets. These outlets include both the open-net and the dark web along with sales platforms, social media, and a variety of payment processors and shipping methods.

National Cyber-Forensics and Training Alliance

HSI has two staff members at the National Cyber-Forensics and Training Alliance (NCFTA), a non-government organization in Pittsburgh, PA. The professionals at NCFTA work with industry and law enforcement to de-conflict leads and coordinate operations between agencies, as well as to share intelligence and develop investigative referrals. The NCFTA brings together experienced law enforcement agents and analysts, governmental experts, and industry leaders to form an integral alliance between academia, law enforcement, and industry.

E-Commerce Working Group

In November 2017, HSI established the E-Commerce Working Group; it includes representatives from various online marketplaces, payment platforms, and express consignment businesses along with CBP and the FBI. This working group also includes the International Anti-Counterfeiting Coalition, a Washington, D.C.-based non-profit organization devoted to combating product counterfeiting and piracy.

The E-Commerce Working Group meets regularly to facilitate the exchange of intelligence, share best practices, and identify cross-sector collaboration among its members. In late 2018, HSI led a pilot project which involved the sharing of data among the participating online platforms. This pilot project demonstrated that criminal organizations are exploiting multiple online platforms to sell counterfeit items.

HSI is also working with members of the E-Commerce Working Group as they strive to establish, by late 2019, a practice of sustained and timely sharing of large amounts of information between the platforms. Once this has been accomplished, the initiative will be expanded to include participation by the payment platforms and express consignment sectors.

Training

HSI offers an advanced commercial fraud training course entitled "Intellectual Property and Trade Enforcement Investigations." This two-week training covers a range of intellectual property and trade enforcement topics. Representatives from the consumer electronics, tobacco, automotive, and other industries subject to high counterfeit risk deliver presentations as part of this training. Four sessions of this course were delivered to 120 HSI and CBP attendees in FY 2019.

13. Appendix D: U.S. Government Efforts

Across the interagency, the USG engages in a comprehensive approach to monitor, deter, and prevent the importation, distribution, and sale of counterfeit and pirated goods into the United States. Law enforcement and regulatory agencies, as well as prosecutors and civil complainants all play a role in addressing this issue, especially as it affects the health and safety, economy and national security of the United States. Some aspects of this approach are mode-neutral while others are specific to the international sale of counterfeit and pirated goods through third-party platforms.

This appendix provides a brief summary of some of the major activities of select agencies and entities to address counterfeits and pirated goods sold on third-party marketplaces. This appendix does not present a comprehensive overview of all efforts to address intellectual property violations.

Department of State

The U.S. Department of State has found that increased diplomatic engagement on intellectual property protections at the highest practical levels, supported by interagency engagement and sustained and targeted capacity building, is an effective way to build up the necessary political will to adequately protect IPR overseas. This diplomatic and capacity-building engagement provides evidence of the weight that the U.S. gives to IPR protection worldwide. High-level engagement on IPR also allows U.S. officials the opportunity to educate foreign officials on the economic, social, and cultural benefits of protecting IPR while at the same time warning of the dangers to their economies, public health, and human safety presented by counterfeits and piracy.

The Department of State, through its Bureau of International Narcotics and Law Enforcement Affairs (INL), in consultation with the Bureau of Economic and Business Affairs Office of Intellectual Property Enforcement, supports the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN).

The GLEN consists of the worldwide deployment of experienced U.S. law enforcement experts to deliver training and technical assistance to foreign law enforcement partners designed to advance operational success. INL also provides assistance to United States Patent and Trademark Office (USPTO) and the DHS IPR Center to enable them to deliver complementary capacity building.

Department of Commerce

The Department of Commerce International Trade Administration's Office of Standards and Intellectual Property OSIP (OSIP) provides domestic outreach events to promote IPR protection in online marketplaces and to educate small and medium sized enterprises on the value of protecting and enforcing their intellectual property rights both domestically and internationally.

Commerce's "STOPfakes Road Shows" represent a unique, interagency outreach event. They are presented in multiple U.S. cities with IPR-intensive industries and provide an array of panel speakers and IPR experts. These Roadshows deliver critically important information about intellectual property to audiences that need it most – start-ups, entrepreneurs, small and medium-sized businesses, independent creators, and inventors.

In addition, OSIP continues to expand the program's unique interactive features. These include guided assistance by CBP officials to assist with trademark recordation and guidance from U.S. Copyright Office officials in registering copyright protections.

USPTO provides policy and technical advice to the Administration and Congress on legislation and other matters relating to civil, criminal, and border enforcement of intellectual property. It is constantly working to improve domestic intellectual property laws and regulations and also seeks to increase public awareness through education on the risks of infringement and the benefits of IPR protection and enforcement.

In 2019, USPTO launched a multi-year, nationwide public awareness campaign with the National Crime Prevention Council in a joint effort to educate U.S. consumers about the dangers of counterfeit goods.

USPTO, including through its Global Intellectual Property Academy (GIPA), provides and participates in technical assistance and capacity-building programs for foreign governments seeking to develop or improve their intellectual property laws and regulations, and to enhance the expertise of those responsible for intellectual property rights enforcement.

Federal Bureau of Investigation

In October 2015, the Federal Bureau of Investigation (FBI) developed a new strategy to combat IPR crime by helping different industry sectors identify common challenges and work together to solve these challenges. The FBI's strategy focuses on building partnerships with key intermediaries in the supply chain for counterfeit and pirated goods, such as e-commerce platforms, payment processors, and the ecosystem for online advertising.

The FBI's strategy also focuses on identifying and pursuing investigations against "systemic enablers" or entities which knowingly facilitate the large-scale infringement of intellectual property rights. As one example of this in action, in 2017 the FBI helped several e-commerce companies re-evaluate their policies regarding the sale of potentially hazardous counterfeit goods online.

At the IPR Center, the FBI helps provide funding and logistical support for the HSI-managed "report IP theft" button, a web-based application for consumers and rights holders to submit complaints to law enforcement regarding suspected infringing activities. The FBI is currently working on developing new analytic tools to help process consumer and rights holder complaints.

U.S. Trade Representative

The Office of the U.S. Trade Representative (USTR) is responsible for developing and coordinating international trade policy for the U.S. government with respect to IPR protections. USTR also oversees negotiations with trading partners, including on IPR issues.

USTR uses a wide range of bilateral and multilateral trade tools to promote strong intellectual property laws and effective enforcement worldwide, reflecting the importance of intellectual property and innovation to the growth of the U.S. economy.

U.S. Food and Drug Administration

The U.S. Food and Drug Administration (FDA) protects the public health by ensuring the safety, efficacy, and security of food, drugs, medical devices, cosmetics and many public health products. One key method that FDA uses to strengthen its public health mission is through regulations and investigations of counterfeit products.

The FDA also issues safety alerts and recalls of dangerous products. The Consumer Product Safety Commission (CPSC) promotes the safety of consumer products by addressing unreasonable risks of injury and developing uniform safety standards. Not surprisingly, counterfeit and pirated products typically do not comply with CPSC requirements.

Consumer Product Safety Commission

CPSC promotes the safety of consumer products by addressing unreasonable risks of injury and developing uniform safety standards. Not surprisingly, counterfeit and pirated products typically do not comply with CPSC requirements.

U.S. Postal Service

As discussed in this report, one critical mission of USPS is to receive advance electronic data (AED) for inbound international mail, originating in 191 different countries. At present, USPS receives AED data from a majority of the inbound international mail it receives. However, it is also required, under the Synthetics Trafficking and Overdose Protection (STOP) Act of 2018, Pub. L. No. 115-271, §§ 8001-8009, 132 Stat. 3893, Title VIII, Subtitle A, to receive AED on all international mail packages by December 31, 2020.

Importantly, USPS provides the its advance electronic data it receives to CBP. This information sharing assists CBP in better targeting packages before the items arrive at the international service centers.

14. Appendix E: Global Initiatives

The proliferation of counterfeit goods on third-party marketplaces is a global problem. This Appendix offers a brief survey of some of the global options and cooperative efforts available to combat the trafficking of counterfeit and pirated goods.

International Organizations

The World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights contains disciplines to protect intellectual property that are enforceable through the WTO's Dispute Settlement Body. The World Intellectual Property Organization, a United Nations specialized agency, is a global forum for intellectual property services, policy, information, and collaboration. The World Customs Organization (WCO) leads international customs cooperation, including with respect to the enforcement of intellectual property rights.

The International Police Organization (INTERPOL), in a partnership with Underwriters Laboratories (UL) operates the International IPR Crime Investigators College (IIPCIC). The mission of IIPCIC is to educate global law enforcement and stakeholder groups to effectively combat transnational IPR crime. Over 160 countries have visited the IIPCIC site since its launch and representatives from over 800 law enforcement agencies have enrolled in the training. INTERPOL enables its members to share and access data on crime and criminals, including counterfeit goods.

Europe

Several European government agencies have developed Memoranda of Understandings (MOUs) with the private sector to address counterfeit issues. For example, the European Commission has facilitated an MOU on the sale of counterfeit goods via the internet with major internet platforms and rights holders who are affected by online sales of counterfeit goods. The platforms commit to notice and take down procedures and to taking pro-active and preventive measures, such as the use of monitoring tools allowing detection of illegal content.

The European Commission also concluded an MOU on Online Advertising and IPR in 2018 that extends to trademarks and copyright. Signatories commit to minimize the placement of advertising on websites and mobile applications that infringe on IPR or disseminate counterfeit goods so as to reduce the revenues of these trafficking websites and apps.

In France, through the French Ministry of Economy, postal operators have signed a charter to address counterfeits with rights holders that focuses on outreach, collaboration and training. In December 2018, brand owners and certain online platforms also signed a charter to fight counterfeits online, which organizes cooperation between brand owners, online platforms, and law enforcement authorities and helps implement preventive measures as well as notice and takedown procedures.

There have also been European efforts to enhance technology associated with protecting intellectual property rights. The European Union Intellectual Property Office (EUIPO) held the

inaugural EU Blockathon competition to develop IPR-protection solutions based on blockchain technologies.

The Intellectual Property Crime Coordinated Coalition (IPC3) at Europol provides operational and technical support to law-enforcement agencies and other partners in the EU. The IPC3 has supported more than 50 high-priority cases of intellectual property infringement. It takes down websites used to sell counterfeit merchandise and shut downs illegal operations that use bitcoin.

The City of London Police (CoLP), and IPR Center partner agency, host the Police Intellectual Property Crime Unit (PIPCU). CoLP is funded by the UK Intellectual Property Office to fight criminals who infringe trademark and copyrights. It works with law enforcement agencies in the UK and across the world to arrest criminals who engage in the production, importation and sale of counterfeit goods.

Postal and customs agencies in France and Italy have organized joint operations where all parcels entering the international office of exchanges from targeted countries are screened for counterfeit goods.

Canada

Canada has created Project Chargeback to fight counterfeiting, fraud, and IPR theft by enabling deceived consumers to get their money back. The initiative, which began in 2012, is administered by the Canadian Anti-Fraud Center (CAFC).

Under the authority of Project Chargeback, defrauded consumers can file a complaint with their bank or the CAFC and provide information on the purchase. The CAFC then works with rights holders to confirm that the goods were counterfeit and relays this information to the cardholder's bank.

The cardholder's bank then initiates a charge back against the seller's merchant account. That results in the termination of the merchant's account used by the counterfeiter, and the victims are instructed not to return the counterfeit goods to the seller.

15. References

Following the mandates set forth in President Trump's April 3, 2019, *Memorandum on Combating Trafficking in Counterfeit and Pirated Goods*, the report shall, as its primary goals:

- Analyze available data and other information to develop a deeper understanding of the extent to which online third-party marketplaces and other third-party intermediaries are used to facilitate the importation and sale of counterfeit and pirated goods;
- Identify the factors that contribute to trafficking in counterfeit and pirated goods; and describe any market incentives and distortions that may contribute to third-party intermediaries facilitating trafficking in counterfeit and pirated goods.
- Identify appropriate administrative, statutory, regulatory, or other changes, including enhanced enforcement actions, that could substantially reduce trafficking in counterfeit and pirated goods or promote more effective law enforcement regarding trafficking in such goods.

In the course of pursuing these goals, the report shall also:

- Evaluate the existing policies and procedures of third-party intermediaries relating to trafficking in counterfeit and pirated goods, and identify the practices of those entities that have been most effective in curbing the importation and sale of counterfeit and pirated goods, including those conveyed through online third-party marketplace
- Identify appropriate guidance that agencies may provide to third-party intermediaries to help them prevent the importation and sale of counterfeit and pirated goods.
- Identify appropriate administrative, regulatory, legislative, or policy changes that would enable agencies, as appropriate, to more effectively share information regarding counterfeit and pirated goods, including suspected counterfeit and pirated goods, with intellectual property rights holders, consumers, and third-party intermediaries.
- Evaluate the current and future resource needs of agencies and make appropriate recommendations for more effective detection, interdiction, investigation, and prosecution regarding trafficking in counterfeit and pirated goods, including trafficking through online third-party marketplaces and other third-party intermediaries; and recommend changes to the data collection practices of agencies, including specification of categories of data that should be collected and appropriate standardization practices for data.
- Identify areas for collaboration between the Department of Justice and Department of Homeland Security on efforts to combat trafficking in counterfeit and pirated goods.

See full memorandum at, President Donald J. Trump, Memorandum on Combating Trafficking in Counterfeit and Pirated Goods, 3 April 2019. https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods/