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

DOGGIE DENTAL INC, *et al*., Plaintiffs, v. ANYWILL, *et al*., Defendants.	Civil Action No. 19-682 (Judge Hornak)
DOGGIE DENTAL INC., *et al.*, Plaintiffs, v. MAX_BUY, *et al*., Defendants.	Civil Action No. 19-746 (Judge Hornak)
DOGGIE DENTAL INC, *et al.*, Plaintiffs, v. GO WELL, *et al.*, Defendants.	Civil Action No. 19-1282 (Judge Hornak)
DOGGIE DENTAL INC, *et al.*, Plaintiffs, v. WORTHBUYER, *et al.*, Defendants.	Civil Action No. 19-1283 (Judge Hornak)

DECLARATION OF STANLEY D. FERENCE III
IN SUPPORT OF MOTION FOR ENTRY OF
DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I, Stanley D. Ference III, hereby affirm as follows:

1. I am over eighteen (18) years of age and not a party to this action. I have never been convicted of a felony or any criminal offense involving moral turpitude, and I am fully competent to attest to the matters stated herein. I have personal knowledge of every statement made in this Certificate of Service and such statements are true and correct.

2. I am an attorney with the law firm of Ference & Associates LLC, which is located at 490 Broad Street, Pittsburgh, Pennsylvania 15143, counsel for the Plaintiffs Peter Dertsakyan and Doggie Dental, Inc. in the above-captioned cases. I make and submit this Declaration in support of Plaintiffs' Motion for Default Judgment and Permanent Injunction (hereinafter "Motion for Default Judgment") against those Defendants for whom the Clerk has entered Default (the "Defendants").

3. Over the past several years, I have reviewed the dockets of over five hundred (500) online counterfeiting lawsuits filed by various brand owners since 2017. It is very rare for any defendant in such a lawsuit to appear, and the lawsuits conclude through the default judgment process.

4. Attached hereto as **Exhibit 1** is a true and correct copy of excerpts of the 2018 Annual Report for Amazon.com, Inc., including excerpts of its Form 10-K for the fiscal year ended December 31, 2018, and available at https://s2.q4cdn.com/299287126/files/doc_financials/annual/2018-Annual-Report.pdf (last visited June 10, 2020).

5. Attached hereto as **Exhibit 2** is a true and correct copy of an article from the Wall Street Journal entitled "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," published on August 23, 2019, and available at

https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990 (last visited June 15, 2020).

6. Attached hereto as **Exhibit 3** is a true and correct copy of an article from the Wall Street Journal entitled "Amazon's Heavy Recruitment of Chinese Sellers Puts Consumers at Risk," published on November 11, 2019, and available at https://www.wsj.com/articles/amazons-heavy-recruitment-of-chinese-sellers-puts-consumers-at-risk-11573489075 (last visited June 15, 2020).

7. Attached hereto as **Exhibit 4** is a true and correct copy of an article from the Washington Post entitled "How Amazon's quest for more, cheaper products has resulted in a flea market of fakes," dated November 14, 2019, and available at https://www.washingtonpost.com/technology/2019/11/14/how-amazons-quest-more-cheaper-products-has-resulted-flea-market-fakes (last visited June 15, 2020).

8. Attached hereto as **Exhibit 5** is a true and correct copy of an article from FoxBusiness.com entitled "Amazon shoppers: Watch out for counterfeit versions of these 17 brand names," dated January 14, 2020, and available at https://www.foxbusiness.com/technology/items-counterfeit-amazon (last visited June 10, 2020).

9. Attached hereto as **Exhibit 6** is a true and correct copy of an article from CNN.com entitled "Fake and dangerous kids products are turning up for sale on Amazon," dated December 23, 2019, and available at https://www.cnn.com/2019/12/20/tech/amazon-fake-kids-products/index.html (last visited June 15, 2020).

10. Attached hereto as **Exhibit 7** is a true and correct copy of an article from The New York Times entitled "Welcome to the Era of Fake Products," dated February 11, 2020, and

available at https://www.nytimes.com/wirecutter/blog/amazon-counterfeit-fake-products/ (last visited June 10, 2020).

11. Attached hereto as **Exhibit 8** is a true and correct copy of an article from the Canadian Broadcasting Corporation entitled "We bought dozens of products from AliExpress, Amazon, eBay, Walmart and Wish. Over half were suspected fakes," dated February 21, 2020, and available at https://www.cbc.ca/news/business/marketplace-counterfeits-fakes-online-shopping-1.5470639 (last visited June 10, 2020).

12. Attached hereto as **Exhibit 9** is a true and correct copy of excerpts of a report issued by the U.S. Customs and Border Protection entitled "Intellectual Property Rights Fiscal Year 2018 Seizure Statistics," and which is available at https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf (last visited June 15, 2020).

13. Attached hereto as **Exhibit 10** is a true and correct copy of an article from CNN.com entitled "Administration wants online retailers to do more to police counterfeit goods," published on January 24, 2020, and available at https://www.cnn.com/2020/01/24/politics/dhs-e-commerce-combat-counterfeit-goods/index.html (last visited June 10, 2020).

14. Attached hereto as **Exhibit 11** is a true and correct copy of a report issued by the U.S. Department of Homeland Security on January 24, 2020, entitled "Combatting Trafficking in Counterfeit and Pirated Goods," and which is available at https://www.dhs.gov/sites/default/files/publications/20_0124_plcy_counterfeit-pirated-goods-report_01.pdf (last visited June 10, 2020).

15. Attached hereto as **Exhibit 12** is a true and correct copy of excerpts of a report issued by the U.S. Trade Representative on April 25, 2020, entitled "2019 Special 301 Report," and which is available at https://ustr.gov/sites/default/files/2019_Special_301_Report.pdf (last visited June 10, 2020).

16. Attached hereto as **Exhibit 13** is a true and correct copy of an article from CNBC.com entitled "How Amazon counterfeits put this man's business on the brink of collapse," published on October 24, 2016, and available at https://www.cnbc.com/2016/10/24/how-amazon-counterfeits-put-this-mans-business-on-brink-of-collapse.html (last visited June 15, 2020).

17. Attached hereto as **Exhibit 14** is a true and correct copy of excerpts from avma.org, the website of the American Veterinary Medical Association, entitled "U.S. pet ownership statistics," and available at https://www.avma.org/resources-tools/reports-statistics/us-pet-ownership-statistics (last visited June 15, 2020).

I declare under the penalty of perjury laws of the United States of America that to the best of my knowledge the foregoing is true and correct.

Executed this 15th day of June, 2020, at Pittsburgh, Pennsylvania.

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

CERTIFICATE OF SERVICE

I hereby certify that on June 15, 2020, the foregoing document is being filed via the Case Management/Electronic Case Filing (CM/ECF) system; I also certify that on the same day, a true copy of the foregoing is being served in accordance with the Order Authorizing Alternate Service.

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

EXHIBIT 1

2018

ANNUAL REPORT

To our shareowners:

Something strange and remarkable has happened over the last 20 years. Take a look at these numbers:

1999	3%
2000	3%
2001	6%
2002	17%
2003	22%
2004	25%
2005	28%
2006	28%
2007	29%
2008	30%
2009	31%
2010	34%
2011	38%
2012	42%
2013	46%
2014	49%
2015	51%
2016	54%
2017	56%
2018	58%

The percentages represent the share of physical gross merchandise sales sold on Amazon by independent third-party sellers – mostly small- and medium-sized businesses – as opposed to Amazon retail's own first party sales. Third-party sales have grown from 3% of the total to 58%. To put it bluntly:

Third-party sellers are kicking our first party butt. Badly.

And it's a high bar too because our first-party business has grown dramatically over that period, from $1.6 billion in 1999 to $117 billion this past year. The compound annual growth rate for our first-party business in that time period is 25%. But in that same time, third-party sales have grown from $0.1 billion to $160 billion – a compound annual growth rate of 52%. To provide an external benchmark, eBay's gross merchandise sales in that period have grown at a compound rate of 20%, from $2.8 billion to $95 billion.

Why did independent sellers do so much better selling on Amazon than they did on eBay? And why were independent sellers able to grow so much faster than Amazon's own highly organized first-party sales organization? There isn't one answer, but we do know one extremely important part of the answer:

We helped independent sellers compete against our first-party business by investing in and offering them *the very best selling tools we could imagine and build.* There are many such tools, including tools that help sellers manage inventory, process payments, track shipments, create reports, and sell across borders – and we're inventing more every year. But of great importance are Fulfillment by Amazon and the Prime membership program. In combination, these two programs meaningfully improved the customer experience of buying from independent sellers. With the success of these two programs now so well established, it's difficult for most people to fully appreciate today just how radical those two offerings were at the time we launched them. We invested in both of these programs at significant financial risk and after much internal debate. We had to continue investing

significantly over time as we experimented with different ideas and iterations. We could not foresee with certainty what those programs would eventually look like, let alone whether they would succeed, but they were pushed forward with intuition and heart, and nourished with optimism.

Intuition, curiosity, and the power of wandering

From very early on in Amazon's life, we knew we wanted to create a culture of builders – people who are curious, explorers. They like to invent. Even when they're experts, they are "fresh" with a beginner's mind. They see the way we do things as just the way we do things *now*. A builder's mentality helps us approach big, hard-to-solve opportunities with a humble conviction that success can come through iteration: invent, launch, reinvent, relaunch, start over, rinse, repeat, again and again. They know the path to success is anything but straight.

Sometimes (often actually) in business, you *do* know where you're going, and when you do, you can be efficient. Put in place a plan and execute. In contrast, wandering in business is not efficient … but it's also not random. It's *guided* – by hunch, gut, intuition, curiosity, and powered by a deep conviction that the prize for customers is big enough that it's worth being a little messy and tangential to find our way there. Wandering is an essential counter-balance to efficiency. You need to employ both. The outsized discoveries – the "non-linear" ones – are highly likely to require wandering.

AWS's millions of customers range from startups to large enterprises, government entities to nonprofits, each looking to build better solutions for their end users. We spend a lot of time thinking about what those organizations want and what the people inside them – developers, dev managers, ops managers, CIOs, chief digital officers, chief information security officers, etc. – want.

Much of what we build at AWS is based on *listening* to customers. It's critical to ask customers what they want, listen carefully to their answers, and figure out a plan to provide it thoughtfully and quickly (speed matters in business!). No business could thrive without that kind of customer obsession. But it's also not enough. The biggest needle movers will be things that customers don't know to ask for. We must invent on their behalf. We have to tap into our own inner imagination about what's possible.

AWS itself – as a whole – is an example. No one asked for AWS. No one. Turns out the world was in fact ready and hungry for an offering like AWS but didn't know it. We had a hunch, followed our curiosity, took the necessary financial risks, and began building – reworking, experimenting, and iterating countless times as we proceeded.

Within AWS, that same pattern has recurred many times. For example, we invented DynamoDB, a highly scalable, low latency key-value database now used by thousands of AWS customers. And on the listening-carefully-to-customers side, we heard loudly that companies felt constrained by their commercial database options and had been unhappy with their database providers for decades – these offerings are expensive, proprietary, have high-lock-in and punitive licensing terms. We spent several years building our own database engine, Amazon Aurora, a fully-managed MySQL and PostgreSQL-compatible service with the same or better durability and availability as the commercial engines, but at one-tenth of the cost. We were *not* surprised when this worked.

But we're also optimistic about specialized databases for specialized workloads. Over the past 20 to 30 years, companies ran most of their workloads using relational databases. The broad familiarity with relational databases among developers made this technology the go-to even when it wasn't ideal. Though sub-optimal, the data set sizes were often small enough and the acceptable query latencies long enough that you could make it work. But today, many applications are storing very large amounts of data – terabytes and petabytes. And the requirements for apps have changed. Modern applications are driving the need for low latencies, real-time processing, and the ability to process millions of requests per second. It's not just key-value stores like DynamoDB, but also in-memory databases like Amazon ElastiCache, time series databases like Amazon Timestream, and ledger solutions like Amazon Quantum Ledger Database – the right tool for the right job saves money and gets your product to market faster.

We're also plunging into helping companies harness Machine Learning. We've been working on this for a long time, and, as with other important advances, our initial attempts to externalize some of our early internal Machine Learning tools were failures. It took years of wandering – experimentation, iteration, and refinement, as well as valuable insights from our customers – to enable us to find SageMaker, which launched just 18 months ago. SageMaker removes the heavy lifting, complexity, and guesswork from each step of the machine learning process – democratizing AI. Today, thousands of customers are building machine learning models on top of AWS with SageMaker. We continue to enhance the service, including by adding new reinforcement learning capabilities. Reinforcement learning has a steep learning curve and many moving parts, which has largely put it out of reach of all but the most well-funded and technical organizations, until now. None of this would be possible without a culture of curiosity and a willingness to try totally new things on behalf of customers. And customers are responding to our customer-centric wandering and listening – AWS is now a $30 billion annual run rate business and growing fast.

Imagining the impossible

Amazon today remains a small player in global retail. We represent a low single-digit percentage of the retail market, and there are much larger retailers in every country where we operate. And that's largely because nearly 90% of retail remains offline, in brick and mortar stores. For many years, we considered how we might serve customers in physical stores, but felt we needed first to invent something that would really delight customers in that environment. With Amazon Go, we had a clear vision. Get rid of the worst thing about physical retail: checkout lines. No one likes to wait in line. Instead, we imagined a store where you could walk in, pick up what you wanted, and leave.

Getting there was hard. Technically hard. It required the efforts of hundreds of smart, dedicated computer scientists and engineers around the world. We had to design and build our own proprietary cameras and shelves and invent new computer vision algorithms, including the ability to stitch together imagery from hundreds of cooperating cameras. And we had to do it in a way where the technology worked so well that it simply receded into the background, invisible. The reward has been the response from customers, who've described the experience of shopping at Amazon Go as "magical." We now have 10 stores in Chicago, San Francisco, and Seattle, and are excited about the future.

Failure needs to scale too

As a company grows, *everything* needs to scale, including the size of your failed experiments. If the size of your failures isn't growing, you're not going to be inventing at a size that can actually move the needle. Amazon will be experimenting at the right scale for a company of our size if we occasionally have multibillion-dollar failures. Of course, we won't undertake such experiments cavalierly. We will work hard to make them good bets, but not all good bets will ultimately pay out. This kind of large-scale risk taking is part of the service we as a large company can provide to our customers and to society. The good news for shareowners is that a single big winning bet can more than cover the cost of many losers.

Development of the Fire phone and Echo was started around the same time. While the Fire phone was a failure, we were able to take our learnings (as well as the developers) and accelerate our efforts building Echo and Alexa. The vision for Echo and Alexa was inspired by the Star Trek computer. The idea also had origins in two other arenas where we'd been building and wandering for years: machine learning and the cloud. From Amazon's early days, machine learning was an essential part of our product recommendations, and AWS gave us a front row seat to the capabilities of the cloud. After many years of development, Echo debuted in 2014, powered by Alexa, who lives in the AWS cloud.

No customer was asking for Echo. This was definitely us wandering. Market research doesn't help. If you had gone to a customer in 2013 and said "Would you like a black, always-on cylinder in your kitchen about the size of a Pringles can that you can talk to and ask questions, that also turns on your lights and plays music?" I guarantee you they'd have looked at you strangely and said "No, thank you."

Since that first-generation Echo, customers have purchased more than 100 million Alexa-enabled devices. Last year, we improved Alexa's ability to understand requests and answer questions by more than 20%, while adding billions of facts to make Alexa more knowledgeable than ever. Developers doubled the number of Alexa skills to over 80,000, and customers spoke to Alexa tens of billions more times in 2018 compared to 2017. The number of devices with Alexa built-in more than doubled in 2018. There are now more than 150 different products available with Alexa built-in, from headphones and PCs to cars and smart home devices. Much more to come!

One last thing before closing. As I said in the first shareholder letter more than 20 years ago, our focus is on hiring and retaining versatile and talented employees who can think like owners. Achieving that requires investing in our employees, and, as with so many other things at Amazon, we use not just analysis but also intuition and heart to find our way forward.

Last year, we raised our minimum wage to $15-an-hour for all full-time, part-time, temporary, and seasonal employees across the U.S. This wage hike benefitted more than 250,000 Amazon employees, as well as over 100,000 seasonal employees who worked at Amazon sites across the country last holiday. We strongly believe that this will benefit our business as we invest in our employees. But that is not what drove the decision. We had always offered competitive wages. But we decided it was time to lead – to offer wages that went beyond competitive. We did it because it seemed like the right thing to do.

Today I challenge our top retail competitors (you know who you are!) to match our employee benefits and our $15 minimum wage. Do it! Better yet, go to $16 and throw the gauntlet back at us. It's a kind of competition that will benefit everyone.

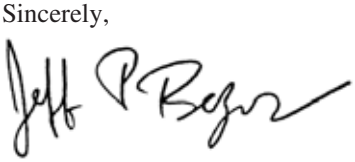
Many of the other programs we have introduced for our employees came as much from the heart as the head. I've mentioned before the Career Choice program, which pays up to 95% of tuition and fees towards a certificate or diploma in qualified fields of study, leading to in-demand careers for our associates, even if those careers take them away from Amazon. More than 16,000 employees have now taken advantage of the program, which continues to grow. Similarly, our Career Skills program trains hourly associates in critical job skills like resume writing, how to communicate effectively, and computer basics. In October of last year, in continuation of these commitments, we signed the President's Pledge to America's Workers and announced we will be upskilling 50,000 U.S. employees through our range of innovative training programs.

Our investments are not limited to our current employees or even to the present. To train tomorrow's workforce, we have pledged $50 million, including through our recently announced Amazon Future Engineer program, to support STEM and CS education around the country for elementary, high school, and university students, with a particular focus on attracting more girls and minorities to these professions. We also continue to take advantage of the incredible talents of our veterans. We are well on our way to meeting our pledge to hire 25,000 veterans and military spouses by 2021. And through the Amazon Technical Veterans Apprenticeship program, we are providing veterans on-the-job training in fields like cloud computing.

A huge thank you to our customers for allowing us to serve you while always challenging us to do even better, to our shareowners for your continuing support, and to all our employees worldwide for your hard work and pioneering spirit. Teams all across Amazon are *listening* to customers and *wandering* on their behalf!

As always, I attach a copy of our original 1997 letter. It remains Day 1.

Sincerely,



Jeffrey P. Bezos
Founder and Chief Executive Officer
Amazon.com, Inc.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to .

Commission File No. 000-22513

AMAZON.COM, INC.
(Exact name of registrant as specified in its charter)

Delaware	**91-1646860**
(State or other jurisdiction of incorporation or organization)	**(I.R.S. Employer Identification No.)**

410 Terry Avenue North
Seattle, Washington 98109-5210
(206) 266-1000
(Address and telephone number, including area code, of registrant's principal executive offices)

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	**Name of Each Exchange on Which Registered**
Common Stock, par value $.01 per share	Nasdaq Global Select Market

Securities registered pursuant to Section 12(g) of the Act:
None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☒

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Smaller reporting company	☐
		Emerging growth company	☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Aggregate market value of voting stock held by non-affiliates of the registrant as of June 30, 2018	$	693,894,417,636
Number of shares of common stock outstanding as of January 23, 2019		491,202,890

DOCUMENTS INCORPORATED BY REFERENCE

The information required by Part III of this Report, to the extent not set forth herein, is incorporated herein by reference from the registrant's definitive proxy statement relating to the Annual Meeting of Shareholders to be held in 2019, which definitive proxy statement shall be filed with the Securities and Exchange Commission within 120 days after the end of the fiscal year to which this Report relates.

including credit and debit cards, we pay interchange and other fees, which may increase over time and raise our operating costs and lower profitability. We rely on third parties to provide certain Amazon-branded payment methods and payment processing services, including the processing of credit cards, debit cards, electronic checks, and promotional financing. In each case, it could disrupt our business if these companies become unwilling or unable to provide these services to us. We also offer co-branded credit card programs, which could adversely affect our operating results if terminated. We are also subject to payment card association operating rules, including data security rules, certification requirements, and rules governing electronic funds transfers, which could change or be reinterpreted to make it difficult or impossible for us to comply. If we fail to comply with these rules or requirements, or if our data security systems are breached, compromised, or otherwise unable to detect or prevent fraudulent activity, we may be liable for card issuing banks' costs, subject to fines and higher transaction fees, and lose our ability to accept credit and debit card payments from our customers, process electronic funds transfers, or facilitate other types of online payments, and our business and operating results could be adversely affected.

In addition, we provide regulated services in certain jurisdictions because we enable customers to keep account balances with us and transfer money to third parties, and because we provide services to third parties to facilitate payments on their behalf. In these jurisdictions, we may be subject to requirements for licensing, regulatory inspection, bonding and capital maintenance, the use, handling, and segregation of transferred funds, consumer disclosures, maintaining or processing data, and authentication. We are also subject to or voluntarily comply with a number of other laws and regulations relating to payments, money laundering, international money transfers, privacy and information security, and electronic fund transfers. If we were found to be in violation of applicable laws or regulations, we could be subject to additional requirements and civil and criminal penalties, or forced to cease providing certain services.

We Could Be Liable for Fraudulent or Unlawful Activities of Sellers

The law relating to the liability of online service providers is currently unsettled. In addition, governmental agencies could require changes in the way this business is conducted. Under our seller programs, we may be unable to prevent sellers from collecting payments, fraudulently or otherwise, when buyers never receive the products they ordered or when the products received are materially different from the sellers' descriptions. We also may be unable to prevent sellers in our stores or through other stores from selling unlawful, counterfeit, pirated, or stolen goods, selling goods in an unlawful or unethical manner, violating the proprietary rights of others, or otherwise violating our policies. Under our A2Z Guarantee, we reimburse buyers for payments up to certain limits in these situations, and as our third-party seller sales grow, the cost of this program will increase and could negatively affect our operating results. In addition, to the extent any of this occurs, it could harm our business or damage our reputation and we could face civil or criminal liability for unlawful activities by our sellers.

Item 1B. *Unresolved Staff Comments*

None.

EXHIBIT 2

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990

Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products

Just like tech companies that have struggled to tackle misinformation on their platforms, Amazon has proven unable or unwilling to effectively police third-party sellers on its site

By Alexandra Berzon, Shane Shifflett and Justin Scheck
Aug. 23, 2019 8:56 am ET

Many of the millions of people who shop on Amazon.com see it as if it were an American big-box store, a retailer with goods deemed safe enough for customers.

In practice, Amazon has increasingly evolved like a flea market. It exercises limited oversight over items listed by millions of third-party sellers, many of them anonymous, many in China, some offering scant information.

A Wall Street Journal investigation found 4,152 items for sale on Amazon.com Inc.'s site that have been declared unsafe by federal agencies, are deceptively labeled or are banned by federal regulators—items that big-box retailers' policies would bar from their shelves. Among those items, at least 2,000 listings for toys and medications lacked warnings about health risks to children.

The Journal identified at least 157 items for sale that Amazon had said it banned, including sleeping mats the Food and Drug Administration warns can suffocate infants. The Journal commissioned tests of 10 children's products it bought on Amazon, many promoted as "Amazon's Choice." Four failed tests based on federal safety standards, according to the testing company, including one with lead levels that exceeded federal limits.

Of the 4,152 products the Journal identified, 46% were listed as shipping from Amazon warehouses.

After the Journal brought the listings to Amazon's attention, 57% of the 4,152 listings had their wording altered or were taken down. Amazon said that it reviewed and addressed the listings the Journal provided and that company policies require all products to comply with laws and regulations.

"Safety is a top priority at Amazon," says a spokeswoman. Amazon uses automated tools that scan hundreds of millions of items every few minutes to screen would-be sellers and block suspicious ones from registering and listing items, using the tools to block three billion items in 2018, she says.

"When a concern arises," she says, "we move quickly to protect customers and work directly with sellers, brands, and government agencies."

Amazon declined to make executives available for interviews.

Christy Stokes blames her son's death on a fraudulently labeled helmet bought on Amazon. Albert Stokes trusted Amazon's quality control, she says, when he picked a motorcycle helmet with an Atlanta Falcons logo for his girlfriend to buy for his 23rd birthday in 2014. It was listed on Amazon as certified by the U.S. Transportation Department.

On June 3, 2014, Mr. Stokes was riding his red Kawasaki in rural Missouri when a Ford Ranger pulled out. He crashed into it, and his helmet came off. A friend phoned his mother to alert her. "When I came up over the hill on the interstate," she says, "there was my son laid out on the highway."

The coroner declared Mr. Stokes dead at the scene, a day before he and his girlfriend planned to find out their unborn baby's gender. His mother sued Amazon, claiming the helmet was flawed. Amazon in court argued it didn't sell the helmet but merely listed it on the seller's behalf. It settled for $5,000 without admitting liability. It declined to comment on the case.

RELATED READING

- Joanna Stern: How to Shop Safely on Amazon
- Read how the Journal analyzed Amazon listings for this article.

The National Highway Traffic Safety Administration said last month that the helmet wasn't DOT compliant and that it had been recalled. It was still listed, and as DOT compliant, last month until the Journal inquired about it, after which Amazon took it down.

Within two weeks of Amazon's removing or altering the first problematic listings the Journal identified, at least 130 items with the same policy violations reappeared, some sold by the same vendors previously identified by the Journal under different listings. Amazon said it then "removed these items and refined our tools to prevent them from being offered in our store."

"There are bad actors that attempt to evade our systems," Amazon said of products in violation of its policies that appear on the site, adding that "should one ever slip through, we work

quickly to take action on the seller and protect customers."

Amazon's struggle to police its site adds to the mounting evidence that America's tech giants have lost control of their massive platforms—or decline to control them. This is emerging as among the companies' biggest challenges.

Amazon, Facebook Inc., Twitter Inc., Alphabet Inc.'s YouTube and others are under scrutiny over how they wield their dominance in booming internet markets while their forums are used for fraudulent listings, offensive content and misinformation—including some spread during America's 2016 elections.

Some lawmakers have begun calling for more regulation of the companies. Courts have begun challenging the firms' interpretation of their legal protections, and regulators are scrutinizing them. Tech companies say they aren't illegal monopolies and have generally pledged to address issues such as misinformation and privacy.

Amazon's legal defense in safety disputes over third-party sales is that it is not the seller and so can't be responsible under state statutes that let consumers sue retailers. Amazon also says that, as a provider of an online forum, it is protected by the law—Section 230 of the Communications Decency Act of 1996—that shields internet platforms from liability for what others post there.

This is similar to a common stance taken by internet companies faced with complaints about content or services offered on their platforms. Courts and regulators have largely agreed—until recently.

SHARE YOUR THOUGHTS

How much oversight should Amazon exert over its third-party vendors? Join the conversation below.

Last month, the U.S. Court of Appeals for the Third Circuit held that a Pennsylvania customer could sue Amazon over an allegedly unsafe product. The court said Amazon could be considered a seller under Pennsylvania law, in part because the company had no vetting process to ensure that third-party sellers were accessible and available for consumers to sue if they were harmed by an item, leaving consumers with no recourse in many cases. The court also held Amazon had considerable control over third-party sellers and could prevent sales of unsafe items. Amazon has asked the appeals court to review the decision.

Last year, the Environmental Protection Agency fined Amazon for letting people sell unregistered pesticides. Amazon agreed, without admitting wrongdoing, to pay a fine and set up new systems to stop such sales. Earlier this year, Washington state's attorney general and Amazon filed a settlement in state court over state allegations that the company allowed school products on the platform that contained lead and cadmium above federal and state limits. Amazon didn't admit wrongdoing.

Amazon tells customers, on its payments site: "We want you to buy with confidence anytime you make a purchase on the Amazon.com website."

On its site aimed at third-party sellers, it says customers "know and trust us, and that trust extends to you."

Third-party sellers are crucial to Amazon because their sales have exploded—to nearly 60% of physical merchandise sales in 2018 from 30% a decade ago, Amazon says. The site had 2.5 million merchants with items for sale at the end of 2018, estimates e-commerce-intelligence firm Marketplace Pulse.

Amazon doesn't make it easy for customers to see that many products aren't sold by the company. Many third-party items the Journal examined were listed as Amazon Prime eligible and sold through the Fulfillment by Amazon program, which generally ships items from Amazon warehouses in Amazon-branded boxes. The actual seller's name appeared only in small print on the listing page.

Customers "could end up in the part of the product pool where who knows where this came from," says Bill Pease, a chief scientist at safety-labeling company UL LLC, who is working with large retailers on setting up new product-safety systems. "And most people don't know that."

Amazon's overriding corporate philosophy of offering ever more options is clashing with internal efforts to make sure product listings won't harm buyers, the Journal found in interviews with former employees and others close to Amazon's safety practices, and from internal records.

The Amazon spokeswoman says: "Our mission is to be Earth's most customer-centric company. We strive for that goal by building the best shopping experience for customers, with unbeatable prices, selection and convenience—but not at the expense of our customers' safety and this insinuation is simply wrong."

To test the effectiveness of Amazon's safety practices, the Journal analyzed listings on Amazon between May and early August, and hired a federally certified testing company to examine certain items bought on Amazon. Among the findings:

•116 products were falsely listed as "FDA-approved" including four toys—the agency doesn't approve toys—and 98 eyelash-growth serums that never undertook the drug-approval process to be marketed as approved.

•43 listings for oral benzocaine, a pain reliever, lacked advised FDA labels warning against use on children under 2.

•80 listings matched the description of infant sleeping wedges the FDA has warned can cause suffocation and Amazon has said it banned.

•52 listings were marketed as supplements with brand names the FDA and Justice Department have identified as containing illegally imported prescription drugs.

•1,412 electronics listings falsely claimed to be UL certified—indicating they met voluntary industry safety standards—or didn't provide enough information to verify the claim.

•The Journal analyzed 3,644 toy listings for federally required choking-hazard warnings. Regulators don't provide databases of toys requiring the warning, so the Journal compared the Amazon listings with the same toys on Target.com and found that 2,324, or 64%, of the Amazon listings lacked the warnings found on the Target listings.

•In addition to the 4,152 items, the Journal initially found 4,510 balloons lacking required choking-hazard warnings listed.

U.S. Public Interest Research Group, a consumer-advocacy organization, in 2018 reported that a large portion of Amazon balloon listings lacked the warning. That Amazon hasn't fixed the problem "shows that Amazon has decided not to put safeguards in place to ensure that kids are protected from one of the largest choking hazards from toys," says Adam Garber, who co-wrote the report. "You can't tell me they can't come up with a system to require companies to include the necessary hazard labels based on what they're selling."

Warnings were added to most listings and a small number were removed after the Journal sent Amazon a list of balloon listings that didn't include the correct language.

Weeks later, the Journal identified an additional 2,208 balloon listings without choking hazard warnings; those, too, now have appropriate warnings or were taken down. Amazon declined to comment on the balloons.

Including the balloons, 83% of the 10,870 total listings the Journal presented to Amazon were taken down or altered. Amazon didn't alter the UL listings. The Amazon spokeswoman says electronics are often rebranded by multiple different sellers that may not be searchable in UL's database.

The Journal's analysis didn't include safety risks of counterfeit products, which some consumers have reported receiving through Amazon. Items disguised as name brands may contain dangerous materials or lack proper warning labels. Amazon says it "strictly prohibits counterfeit goods."

Dozens of products the Journal identified as dangerous or mislabeled had the Amazon's Choice designation, which many consumers take to be Amazon's endorsement. The company's website says Amazon's Choice reflects a combination of ratings, pricing and shipping time.

One was the toy musical-instrument set Darice Taipalus bought her son in March when he was 16 months old, she says. The Texas database developer says she assumed everything on Amazon met safety standards, until the Journal contacted her.

The Amazon listing said the set was "made of high quality nontoxic material, safe and reliable for little children" and claimed approval from the FDA. Journal-commissioned testing showed the set's xylophone contained nearly four times the lead the federal government allows in children's products. According to the testing company, the set also failed tests based on federal requirements for determining sharp points.

"He's a toddler," Ms. Taipalus says. "Everything goes in his mouth." She says she threw the set away after hearing the Journal's testing results.

Amazon initially didn't take the product down after the Journal informed it of the test results, saying a Chinese entity that goes by the name Ailuki had previously provided a test report showing there were no detectable lead levels. It subsequently took the set down in the U.S. and says it is asking Ailuki for more documentation.

Ailuki sent the Journal a test report it said it had commissioned that stated there were no detectable lead levels. It didn't respond to further requests for comment.

Another musical-instrument set failing the Journal's tests, made by a company calling itself Innocheer and listed as in China, likely contributed to a New York City child's lead poisoning, according to city health officials. The city in May 2018 began tracking down contaminated products including the set bought on Amazon, a New York health-department spokesman says.

Subsequent testing showed the set's bright-yellow maracas contained 411 times the lead legally allowed, health-department documents show. After a federal recall last fall, Amazon pulled the listing and notified customers of the recall, the company says. "We execute recalls as soon as we are aware of them," it says.

The set later appeared online with red maracas, stating the instruments were lead-free. In the Journal-commissioned tests, conducted after the recall, the maracas didn't contain lead but

other instruments in the set failed sharp-point tests. Innocheer couldn't be reached for comment. Amazon has taken the set down in the U.S., saying it is requesting additional compliance documentation.

In its early days, Amazon operated a lot like big-box stores, largely in direct control of its supply and distribution chains. Customers got products directly from Amazon or a known retail partner such as Toys "R" Us. In 2001, third-party sellers made up 6% of Amazon's physical merchandise sales, company data show.

The same year, the company articulated a core philosophy that helped spur the growth of third-party sellers. According to published company histories, founder Jeff Bezos and other officials scribbled an image of a "virtuous cycle": It depicted how third-party vendors would want to sell to Amazon's customers and would add more products at less expensive prices, attracting even more customers and more sellers.

As smaller retailers joined Amazon's marketplace, the company seemed unprepared to police them, some former employees say. In 2011, a team of three oversaw safety for the entire site, which essentially consisted of managing recalled products, say some of them, including Rachel Johnson Greer, a former employee who managed Amazon's safety systems until 2015 and now advises third-party Amazon sellers.

The main enforcement effort on product safety was rudimentary and involved running an Excel spreadsheet script to identify products recalled by the consumer-safety commission and manually then remove them, Ms. Greer and the other former employees say.

Many risky products got through, and the third-party marketplace became "a giant disaster zone," says Ms. Greer. "It was absolutely insane." Ms. Greer says she worked initially with an engineer and legal intern to develop a machine-learning tool to automatically take down restricted products. It scanned third-party-item descriptions for certain keywords, growing smarter as the team refined what to target, she says.

The safety team grew rapidly alongside the artificial-intelligence tool, with hundreds of people across several departments and countries. But product volume was growing, and many products continued to slip through, she and other former employees say.

At one point in 2013, some Amazon employees began scanning randomly selected third-party products in Amazon warehouses for lead content, say people familiar with the tests. Around 10% of the products tested failed, one says. The failed products were purged, but higher-level employees decided not to expand the testing, fearing it would be unmanageable if applied to the entire marketplace, the people familiar with the tests say. Amazon declined to comment on the episode.

"Amazon will always default to allowing more stuff to be available to the customer," says Ms. Greer. In 2017, she ordered baby products, children's toys and food-related products from Amazon that came up high in search results but had false certification claims, such as claiming FDA approval, and sent them to federally certified laboratories for testing. She says that, at the time, she estimated 80% of Amazon's third-party sellers didn't comply with federal, state or industry safety and labeling standards and that the vast majority of the issues were not having proper warnings and labels.

The Amazon spokeswoman calls Ms. Greer's analysis "wrong and baseless" and says Amazon doesn't sacrifice product safety in favor of selection. Ms. Greer says she stands by her analysis.

Amazon doesn't do its own testing for product safety, according to documents the company filed in the Washington-state case. It does sometimes randomly buy certain high-end jewelry and send it out for testing to make sure third-party sellers aren't peddling fake jewels, according to its publicly posted procedures. The Amazon spokeswoman says the jewelry spot tests are one of various programs the company does to "ensure customers receive the compliant products they expect."

Amazon openly encourages anyone to sign up and start selling right away unless something in their registration or initial posting triggers the automated tools to flag them for more vetting.

In contrast, Walmart Inc. requires all products on store shelves be tested at approved labs, company documents show. Target says it requires suppliers of store-branded products to undergo additional inspections and testing beyond government standards.

Target and Walmart have created online marketplaces for third parties to sell directly to consumers. Target's site, launched earlier this year with several sellers, is invitation-only. Walmart had around 22,000 sellers at the end of 2018, according to Marketplace Pulse. It requires an application that can take days for approval, and only a fraction of merchants applying make it through the vetting, says a person familiar with Walmart's policy.

The Journal didn't analyze products sold on Walmart and Target shelves or websites.

A persistent problem for Amazon has been magnetic toys. Amazon and other big retailers banned sets of high-powered magnetic balls and cubes in 2012 after reports of thousands of children ending up hospitalized for swallowing them. Inside the body, the magnets can snap together and rupture abdominal tissue. The Consumer Product Safety Commission, or CPSC, has called them a "substantial product hazard." Retailers still selling them generally allow them on store shelves only when marketed for adults.

Amazon's policy said it prohibited "Products that include large quantities of magnetic balls or cubes, such as:" then listed eight brands. But knockoffs of the toys slipped through. The Journal

found nearly 80 that appeared to match listings of the banned toys. About 40 of these listings were removed after the Journal contacted Amazon. Roughly 30 still remain that appear to match descriptions of prohibited products originally described on Amazon's compliance pages.

Danny Puskarcik, who worked in product compliance at Amazon until early this year, says the magnets issue "was an extremely high priority," seen as so serious that employees sought to enforce the policy very broadly. "The idea was to catch all powerful magnets," he says. "Get rid of them. Destroy them."

Creed Cameron, an Amazon manager for restricted products until 2017 and no longer at the company, says his team never found a good way to handle the magnet problem. Taking down the cheap, mass-manufactured products, he says, was "like trying to stop a bullet."

After the Journal contacted Amazon about the knockoffs, the spokeswoman said that despite the wording of the policy—and the experiences described by the two former workers—the company intended to ban only the specific magnet-toy brands listed. Other magnet toys, including ones identical to the banned toys but sold under different names, were supposed to be allowed on the site, she said.

Amazon then changed the wording of the policy to ban the specific brands. The spokeswoman declined to comment on why Amazon has banned some brands but not others.

Amazon's policy of banning only some brand-name products "makes no sense," says Alan Schoem, a lawyer who has represented one of the banned brands and is a former CPSC official. "You'd think they'd want to be a little more careful."

When Amazon does take down listings for banned items, the same products sometimes reappear under new accounts, the Journal found.

The EPA has announced a ban starting in November on consumer products containing methylene chloride, which the agency has linked to cancer and sudden death from toxic fumes. Amazon late last year said it would purge paint strippers using the chemical by March, but there were still dozens of them for sale then. When an advocacy group named Safer Chemicals, Healthy Families identified the products, Amazon took them down.

More such paint strippers popped up and were removed only after the group flagged them. "They clearly need to do a better job of setting up a system to police their supply chain," says Mike Schade, a campaign director for the nonprofit. Amazon declined to comment on the paint strippers.

Neither Amazon nor federal regulators have made public attempts to measure the scale of the site's safety issues, but at least one state has done so for one product category. This year, the Washington state attorney general's office examined school supplies and found 35 out of 41

Amazon products tested contained amounts of cadmium, lead or both above federal or state limits, state documents show.

Discount stores that the state studied also had a similar ratio of problem products, while other retailers in the test didn't, says Kelly Wood, one of the state attorneys involved in the case.

After the state notified Amazon, the company conducted tests in a warehouse and found that four of 45 tested items had hazardous levels of lead or cadmium, including a unicorn necklace whose pendant-backing makeup was 35% cadmium, more than 8,500 times the legal limit in Washington, state documents show.

Washington state asked Amazon to provide documentation for the children's products showing they had passed safety tests outlined in the company's internal policies. Amazon told the state the company may request certificates for certain high-risk products, and that any seller is required to provide them when asked, but that it didn't have any for the products identified by the state.

Even after Amazon, prompted by the state, went to retailers and asked them directly for the compliance documents and certifications, it didn't receive documents back, the company said, according to documents obtained by the state.

"They weren't really checking that these products were tested prior to putting them up on their website," says Mr. Wood.

The Amazon spokeswoman says the company "worked with our selling partners to verify that the school supplies and children's jewelry in our store are safe and enhanced our processes to verify the safety of these products moving forward. We welcome ongoing collaboration with the Attorney General and other agencies to promote customer safety."

Amazon customers the Journal contacted who bought products that didn't meet safety standards say they had assumed they were buying from Amazon directly or that everything on the website passed safety standards.

That includes Ms. Stokes, whose son died in the motorcycle accident wearing a helmet falsely claiming DOT compliance. She sued Amazon, the Ford Ranger driver and Ivolution, the Corona, Calif., company that sold the helmet, in Missouri state court, alleging that the truck driver was at fault for the accident and that the helmet had a faulty strap. The driver settled. The case against Amazon and Ivolution was moved to federal court in the Western District of Missouri.

Ivolution owner Ricky Zhang in court statements said another man had bought 103 helmets from him and sold them on Amazon and that Ms. Stokes didn't prove the accident was related to

the helmet. His company bought products from China to resell on Amazon, according to the legal documents. It was so small he couldn't afford legal representation, he said in court.

The judge ordered Ivolution to pay $1.9 million to Mr. Stokes's family, which says the company hasn't done so. Mr. Zhang didn't respond to requests for comment.

Amazon attorney Monte Clithero says the company, which settled the case for $5,000, denies any responsibility. "Basically, a third party was using Amazon as a bulletin board to advertise the product and sell."

On July 1, 2019, the National Highway Traffic Safety Administration said Ivolution had recalled the helmet—it said 4,071 were on the market or sold. An agency test in April 2018 had found the helmet cracked open on contact.

On July 29, the helmet model and eight other helmets that failed federal safety tests in 2018 were still listed for sale on Amazon. Amazon removed them after the Journal pointed them out.

A week later, the Journal found a listing for the helmet model Mr. Stokes wore was listed on Amazon by a different vendor, labeled as out of stock. There were also listings for four other helmets Amazon had taken down after the Journal notified it that the products had failed federal safety tests.

Amazon then took those down.

— Lisa Schwartz and Fanfan Wang contributed to this article.

—Additional design and development by Angela Calderon, Joel Eastwood, Jessica Kuronen, and Allison Pasek

Write to Alexandra Berzon at alexandra.berzon@wsj.com and Justin Scheck at justin.scheck@wsj.com

Copyright © 2020 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

EXHIBIT 3

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/amazons-heavy-recruitment-of-chinese-sellers-puts-consumers-at-risk-11573489075

Amazon's Heavy Recruitment of Chinese Sellers Puts Consumers at Risk

The e-commerce platform has included banned, unsafe, mislabeled products. One reason: It wooed China's manufacturers to sell directly to the U.S.

By Jon Emont
Nov. 11, 2019 11:17 am ET

It looked like Amazon.com Inc.'s yearslong quest to build a shopping business in China was a bust in July when it folded a big part of its local business.

In fact, Amazon's China business is bigger than ever. That is because it has aggressively recruited Chinese manufacturers and merchants to sell to consumers outside the country. And these sellers, in turn, represent a high proportion of problem listings found on the site, according to a Wall Street Journal investigation.

The Journal earlier this year uncovered 10,870 items for sale between May and August that have been declared unsafe by federal agencies, are deceptively labeled, lacked federally-required warnings, or are banned by federal regulators. Amazon said it investigated the items, and some listings were taken down after the Journal's reporting.

Of 1,934 sellers whose addresses could be determined, 54% were based in China, according to a Journal analysis of data from research firm Marketplace Pulse.

Amazon's China recruiting is one reason why its platform increasingly resembles an unruly online flea market. A new product listing is uploaded to Amazon from China every 1/50th of a second, according to slides its officials showed a December conference in the industrial port city of Ningbo.

Chinese factories are squeezing profit margins for middlemen who sell on Amazon's third-party platform. Some U.S. sellers fear the next step will be to cut them out entirely.

Tony Sagar began noticing the China effect around 2015. His company, Down Under Bedding in Mississauga, Ontario, had sold goose-down duvets on Amazon since 2014—these days, for $699 for a queen-size version. Then Chinese competitors hit, listing goose-down duvets for

sometimes a sixth his price. He bought one and had it tested: Inside was inexpensive duck down.

The Journal in October bought a duvet from the same Amazon seller claiming "100% Fill With Goose Down" and had it tested. The result matched Mr. Sagar's: duck feathers.

"They're claiming they're selling a $500-$700 duvet based on false specifications, so people say, '$120, it's a good deal!' " Mr. Sagar said. "Amazon is making a direct push for these factories in China."

AMAZON'S UNRULY MARKETPLACE

- Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products
- VIDEO: How Scammers in China Manipulate Amazon
- Amazon Sells Clothes From Factories Other Retailers Blacklist

In response to this article, an Amazon spokesman said, "Bad actors make up a tiny fraction of activity in our store and, like honest sellers, can come from every corner of the world. Regardless of where they are based, we work hard to stop bad actors before they can impact the shopping or selling experience in our store."

Amazon said it took enforcement action on the duvet seller and that its products were no longer for sale on the site. The seller's listings appeared to be gone from Amazon's U.S. site as of last week.

Mr. Sagar's discovery came as Amazon was expanding a campaign it started around 2013 urging Chinese businesses to sell directly to consumers abroad. An Amazon sales director, Alicia Liu, at a 2017 conference told Chinese business people she was leading a team in China, drawing on her previous experience cutting out middlemen in Walmart Inc.'s supply chain.

"We help factories directly open accounts on Amazon and sell to U.S. consumers directly," a video shows her telling them. "This is our value."

A wave of Chinese merchants have joined Amazon's millions of third-party sellers worldwide, who collectively represent more than half of Amazon's physical gross merchandise sales.

Among the 10,000 most-reviewed accounts on Amazon's U.S. site whose locations could be determined in October, about 38% were in China, Marketplace Pulse calculates, compared with 25% three years ago.

The Amazon spokesman said 38% "is a significant exaggeration of the real percentage of the top ten thousand'' and that the methodology is flawed, citing what it said were problems with the way in which the analysis used seller review counts to estimate the percentage. Marketplace Pulse said it stood by its analysis.

Site control

How Amazon exercises control of its site has come under scrutiny from some in Congress, where some lawmakers are calling for more regulation of the company. That is part of a growing backlash in Washington over how tech companies run their platforms.

Amazon's third-party marketplace, which connects merchants and buyers around the world, is crucial to the company's growth. At the same time, even though it has become a source of fake or dangerous goods, Amazon has denied it is liable for what's sold there, saying in court cases that it neither makes nor sells the products in question.

In its annual Securities and Exchange Commission filing this year, Amazon disclosed for the first time that counterfeits and fraudulent products are a risk factor. It said Amazon may be "unable to prevent sellers in our stores or through other stores from selling unlawful, counterfeit, pirated, or stolen goods," among other issues.

Amazon said it recruits sellers in many countries and that these merchants are central to its goal of offering customers good selection at good prices. Amazon said it requires products to comply with applicable laws and regulations. It said that in 2018 it blocked more than three billion suspect listings for various forms of abuse.

Consumers and businesses with safety and intellectual-property grievances have found it hard to hold Chinese sellers accountable—in part because Amazon doesn't require its sellers to provide their locations to the public on its U.S. site.

The Journal identified sellers as being in China from their pages on Amazon's site in Mexico, where regulations require sellers to list their locations on Amazon—a method Marketplace Pulse also uses.

New sellers from China are hurting merchants that have built Amazon businesses offering products they import from Chinese factories, said Amazon seller Bernie Thompson. His Plugable Technologies in Redmond, Wash., lists electronics products made in China. Since about five years ago, Chinese manufacturers selling on Amazon have priced him out of some product categories, he said—some of them his own suppliers and others who game Amazon's rating system, he said.

"Amazon is trying to disintermediate everyone they can, and get products as directly as possible to consumers," he said. "In a way, they're a perfect partner for China Incorporated to

engage with to take them around the world."

The Amazon spokesman said: "Independent retailers in the U.S. are enjoying record sales in our store." Amazon said more than 75% of the 10,000 top sellers by gross sales in its U.S. store were America-based as of 2018 and that the company spends more recruiting U.S. sellers than sellers from any other location.

Global recruiting

In China over the past six years, Amazon has made its site more accessible to Chinese speakers, created special programs that address Chinese sellers' logistical needs and sent a stream of employees to recruit suppliers.

Amazon 'is the most cost-effective way to sell into the United States,' says businessman Zhao Weiming. A factory in southern China produces his Lagunamoon-branded products.

PHOTO: BILLY H.C.KWOK FOR THE WALL STREET JOURNAL

At the 2017 conference, Ms. Liu, who said she had spent over a decade purchasing for Walmart, told Chinese sellers that when she joined the industry in 2004, around 90% of her suppliers were trading companies and that by 2017, around 80% were the factories themselves. Ms. Liu said the same logic applied to Amazon, the video shows.

"Let's cut out the middleman," said Geoffrey Stewart, an Amazon employee in Shenzhen, at an April trade event in Hong Kong in a video the Journal viewed. "We think that will enhance margins for our manufacturing partners and it will delight customers."

Amazon said Ms. Liu's and Mr. Stewart's comments didn't mean Amazon was less committed to helping sellers everywhere. Ms. Liu, who no longer works at Amazon, didn't respond to LinkedIn messages, and the Journal couldn't determine where she now works. Amazon said Mr. Stewart wasn't available for comment. Walmart declined to comment on Ms. Liu's assertions.

Amazon seller Zhao Weiming said the site "is the most cost-effective way to sell into the United States." The Guangzhou businessman experimented several years ago listing gadgets on Amazon before settling on cosmetics and essential oils, he said, establishing factories to produce them under the name Lagunamoon. He said his company earns $50 million a year on Amazon.

Listings for some popular Lagunamoon essential oils claimed they were U.S. Food and Drug Administration approved, until the Journal raised the matter with Amazon and Mr. Zhao in early November. An FDA spokesman said essential oils wouldn't meet the agency's definition of an approved product, although it was possible some component—a dye, say—might be approved.

Mr. Zhao said FDA requirements are complex and he didn't want to use tens of thousands of words to explain.

Amazon said it was investigating the case and would take proper action. It said sellers are prohibited from listing products that improperly claim to be FDA cleared or FDA approved, or improperly include the FDA logo. At least one Lagunamoon essential-oil listing that cited FDA approval had that claim removed after inquiries from the Journal.

Concerns at Amazon about Chinese listings arose several years ago in its China team, which noticed that as local sellers flocked to the platform, it saw increasing patterns of fraud, counterfeits and unsafe products, said former Amazon employees in China.

Washington state's attorney general's office said Amazon agreed to pay $700,000 as part of a legally binding agreement after an investigation revealed dozens of products marketed toward children had excessive lead and cadmium. The products were made in China, the office said, some sold by China-based third parties. Amazon didn't admit wrongdoing.

"Customer safety is Amazon's top priority," said the Amazon spokesman. "We work closely with our selling partners to verify that the school supplies and children's jewelry in our store are safe."

Bogus brushes

Cheap Chinese counterfeits drove Kevin Williams, a Utah seller of water-powered cleaning brushes on Amazon, to lay off six employees this year—most of his U.S. staff, he said. He and his co-founder developed their patented Brush Hero product, made in the U.S. and U.K., in 2015 after finding it difficult to clean their vehicles, selling them on Amazon for $34.99.

Kevin Williams, co-owner of Brush Hero, at his distribution warehouse in Salt Lake City, Utah on November 8, 2019.

PHOTO: LINDSAY D'ADDATO FOR THE WALL STREET JOURNAL

Poorly made copies began appearing in 2018 on Amazon, eventually listing for as low as $9.99, some claiming to be the Brush Hero brand, he said. Buyers, unaware they were fake, trashed Mr. Williams's products on his Amazon page, he said. When he complained to Amazon, he said, it told him to order the alleged counterfeits and test them. Amazon removed brushes he proved counterfeit, he said, but it could take weeks for them to arrive for testing, and new counterfeits kept popping up.

He dropped prices to $19.99, which "pulled out the rug from us from a cash-flow perspective" he said. A retailer declined to give him a large contract. "He said, 'What the heck, your Amazon reviews are terrible,' " said Mr. Williams, who calls his company "walking dead."

Amazon said that it acted on infringement cases where Brush Hero provided adequate information and that it has introduced programs for sellers to fight counterfeits, including one called Project Zero that uses automation to scan Amazon stores and remove suspected counterfeits.

Counterfeits and inauthentic reviews "have all gone through the roof with the rise of Chinese sellers," said Chris McCabe, an investigator for Amazon until 2012, now a consultant helping Amazon sellers counter illicit competition.

Inauthentic reviews for listings from China can trick Amazon's algorithm into boosting products, people outside Amazon familiar with the activities said. A search for "travel pillows" in August presented products with names such as MLVOC offered by sellers whose names matched those of Amazon accounts registered in southern China.

The Journal ordered MLVOC-brand pillows from sellers named Corki and Kingstyle Supplies, and got gift cards offering a free pillow if the buyer emailed an address—the same address for both sellers. A "Gift card team" responded, asking the buyer to give a five-star review for which it promised an Amazon gift card. Of one MLVOC pillow's roughly 2,000 reviews, about 86% have five stars.

Amazon policy forbids making inducements for positive reviews. Amazon said it investigated and took action, eventually reinstating Kingstyle and Corki. Amazon said in some cases it will reinstate seller accounts after violations if the sellers provide corrective action plans, though the accounts would be blocked after further infractions.

SHARE YOUR THOUGHTS

Do you care what country your Amazon seller is in? Join the conversation below.

In response to a query sent to the email address given by Corki and Kingstyle, a respondent wrote: "I can't share the company information." The sellers didn't respond to requests for comment sent through Amazon's platform.

Travel-pillow seller Teri Mittelstadt, co-founder of HiGear Design Inc. in California, said counterfeits and review manipulation from China have hurt sales. Her patented Travelrest pillows, which attach to airline seats to prevent slipping, were among the top-selling travel pillows on Amazon for seven years starting in 2008, she said, but now rank in the 20s or lower.

"The person who gets hurt the most is the consumer who buys the product. They think they are buying a product with all these great reviews," she said.

Amazon said Travelrest's sales on Amazon have steadily grown year-to-year since 2015. Ms. Mittelstadt said her sales growth has slowed significantly over the past two years and that this year her sales are down on Amazon's U.S. site.

Strategy shift

Starting in the mid-2000s, Amazon's attempt to build an online retail business in China was thwarted by local competitors like Alibaba. Early this decade, it began experimenting with the new strategy, and employees "realized that global selling is much bigger" than selling in China, a former Amazon manager said.

At a Shenzhen trade fair in early 2013, no one had heard of Amazon, said Steven Chen, who says Amazon dispatched him to recruit Chinese sellers. He left Amazon in 2015 and operates an e-commerce consulting business.

Amazon employees distributed Chinese-language tutorials on opening Amazon accounts to prospective new sellers, people familiar with the company's strategy said. Interns in Beijing phoned vendors on Chinese e-commerce sites to invite them to join Amazon.

Chinese sellers' products often took weeks to ship across the Pacific and arrive at buyers' addresses. So Amazon offered a logistics system, "Dragonboat," which for a fee brought goods made in China and elsewhere to Amazon fulfillment centers in the U.S.

American buyers could receive purchases within 48 hours in Amazon boxes, said a former high-level Amazon China employee and a Chinese seller who used the service.

By 2015, Amazon's website was functional for sellers in Mandarin. Its team responsible for signing up and assisting Chinese sellers expanded to 120 people in 2016, said the former high-level employee. Other employees built relationships with businesses such as Chinese logistics-services providers and translator services, asking them to encourage clients to establish Amazon accounts.

It is often hard to tell that an Amazon seller is based in China, as is the case with the Amazon page of Lagunamoon, the essential-oil and cosmetics provider. It shows no indication the products are Chinese and gives no store address. Lagunamoon's Mr. Zhao said that is because the U.S. doesn't require it.

Amazon seller Molson Hart in Texas is suing 73 sellers, many located in China, in Texas federal court, for trademark infringement on products like his Brain Flakes interlocking plastic disk set. He has been selling the Chinese-made toys on Amazon since 2014, and counterfeits started appearing in 2015, he said.

After he filed suit, he couldn't hunt down the Chinese companies. "I know who did it," he said, "but I can't serve them."

Amazon said it has worked closely with brands to support criminal referrals against counterfeiters in China and anticipates working with brands to jointly pursue litigation in the U.S. and China.

Amazon buyer Irvin R. Love Jr. of Georgia bought a hoverboard on Amazon in November 2015 that caught fire and burned down his home, according to a suit he filed February 2018 against Amazon, the seller and others, in Georgia federal court. In an amended complaint this year he alleged that Amazon was negligent for not removing the hoverboard from its website before Mr. Love's purchase. Amazon argued in a legal filing that it doesn't owe damages because it didn't design, manufacture or sell the hoverboard.

Mr. Love also sued the seller, Panda Town, which his lawyer, Darren Penn, said appeared to be a Chinese company, based on sales information. Mr. Penn said that he can't locate the seller and that Amazon declined to provide its location.

Cross-border e-commerce has made it harder to police unsafe products entering the U.S., he said. "When you had the traditional importer and customs and brokers—and all those procedures are followed—you provide a couple of layers of protection that you don't when you're talking about an internet market." The case is in discovery, and Mr. Penn declined to make Mr. Love available for comment.

Amazon said it has provided information about the seller to the plaintiff, consistent with its policy on such matters. Panda Town doesn't appear to list on Amazon anymore, and the Journal couldn't locate a company by that name.

'Not normal'

Product safety on Amazon and other online marketplaces isn't assured, because Amazon doesn't require all third-party sellers to test products to prove they are compliant with regulations, said Sebastien Breteau, chief executive of QIMA, an inspection, certification and audit company that is an Amazon vetted service provider.

"It's not normal that a factory with 200 people manufacturing baby monitors in Dongguan can ship products directly to consumers in Minnesota or in Europe through a marketplace," he said. "The day the regulator makes them responsible, then we'll have proper compliance programs."

Amazon said sellers create their own product listings and are required to comply with all relevant laws and regulations when listing items for sale in Amazon stores.

Mr. Thompson, the electronics seller, said Chinese factories have steadily pushed him out of lower-end goods such as USB cables, pricing at less than he can. The Chinese sellers often boost their product rankings by arranging large purchases of their own products and leaving positive reviews for themselves, he said—a tactic he said he learned about while attending an independent Amazon-seller event featuring a China-based sales consultant in Hong Kong several years ago.

He now counts on selling higher-end products like $199 docking stations for displays and charging electronic devices, he said, but "there really isn't much upper end left for us."

Amazon said competition is a part of business and some more-mature product categories can be particularly competitive. The spokesman said its goal is to quickly remove abusive reviews and that over the past month "over 99% of the reviews read by customers were authentic."

Chinese sellers were seen as too valuable to give up, despite warning signs, a former Seattle-based Amazon employee said. "There were crazy things, hundreds of listings created every

hour," the person said, adding that when U.S. vendors complained, staff told them, "We don't control third-party selection. It's not us, it's an open-end platform."

Goose-down test

Mr. Sagar, the goose-down-duvet seller, said an employee posing as a customer last year contacted Rosecose, the Chinese seller of the down duvet on Amazon, offering proof its product was deceptively listed. A Rosecose representative apologized and said its suppliers could be to blame, offering to refund the lab-test costs, according to messages the Journal viewed.

The employee last year also sent an email to Amazon with the test results showing the duck down, he said. Rosecose kept listing duvets, Mr. Sagar said.

The Journal bought a duvet on Amazon from Rosecose in October and sent its own test results to Amazon late in the month. Early this month, Rosecose was still selling duvets on Amazon as "100% Fill With Goose Down," including a king-size option listing for $129.99.

The Wall Street Journal verified Rosecose was based in China by visiting its page on Amazon's Mexican site, which listed its location. Rosecose didn't respond to inquiries sent through Amazon and no one picked up calls to a phone number associated with the brand.

Amazon said it took down Rosecose listings Nov. 4. They appeared to be gone from the U.S. site early last week, but some still appeared on Amazon's Canada site until after the Journal pointed them out to the company.

—Shane Shifflett, Stella Yifan Xie and Lekai Liu contributed to this article.

—Illustration by Jessica Kuronen/WSJ

Write to Jon Emont at jonathan.emont@wsj.com

Copyright © 2020 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

EXHIBIT 4

The Washington Post

Technology

How Amazon's quest for more, cheaper products has resulted in a flea market of fakes

Former executives say e-commerce giant, which last year spent $400 million fighting fraud and abuse, has prioritized its broad selection over anti-counterfeiting

By Jay Greene
November 14, 2019

Hermès's $640 Clic H Bracelet is one of those luxury baubles that's financially out of reach for most shoppers. So how is it that Amazon shoppers could recently search for the Hermès piece by name and find a bracelet for just $24.99 on the e-commerce giant's website?

The version on Amazon has the same clasp with an Hermès "H" logo that flips up to open the bracelet, as well as its name etched on the inside. But Amazon's version, sold by a third-party merchant, is fake. If the price isn't a giveaway, the product reviews should be. "People probably can't tell the difference between this and the real one from far away. I must admit they really did a great job for the dupe!" one buyer wrote in September.

Amazon executives have publicly lamented the scourge of counterfeits, saying they have spent hundreds of millions of dollars and hired thousands of workers to police its massive market of third-party firms that use the e-commerce site to sell their goods. But as the availability of the fake Hermès bracelet shows, Amazon's system is failing to stanch the flow of dubious goods even with obvious examples of knockoffs.

The continued abundance of counterfeit goods on the site is the result of Amazon's decisions to prioritize a broad selection of products and cheaper prices over the deployment of aggressive technologies and policies that could further stem the problem, according to former executives and outside consultants.

Amazon relies on brands to let the company know about frauds, but even when the company has custody of counterfeit items, it doesn't always take action. Scads of counterfeit products, including the Hermès bracelet, land in Amazon warehouses before they're shipped to consumers. But Amazon very rarely inspects them for authenticity.

The Seattle-based e-commerce giant keeps a roughly 15 percent cut of the sales of third-party sellers regardless of whether the product is counterfeit. But losing out are not just luxury brands — many of the counterfeit products include safety items, baby food and cosmetics, according to recent testimony to the Commerce Department, which is probing counterfeit sales online.

When Amazon stepped up efforts to curb its counterfeit problem two years ago, complaints from shoppers fell, one of the former Amazon executives said. But so did the rate at which the company expected its product selection to grow, the person said. So in early 2018, Amazon began aggressively adding merchants, regardless of whether they were authorized by brands to sell their products, the former executive said.

“Because they are allowing so much onto the site, they can’t handle the manual follow-up these things require,” said the former executive, who spoke on the condition of anonymity to avoid reprisals. “It tells me they just don’t want to find it. They want the selection.”

Amazon goes “well beyond our legal obligations” to snuff out fakes on the site, spokeswoman Cecilia Fan said. In addition to staff that investigates fraud claims, the company has developed algorithms to sift through the more than 5 billion changes to its worldwide catalogue each day, she said. For every case reported, the company blocked or removed over 100 proactively with its systems, she said.

(Amazon chief executive Jeff Bezos owns The Washington Post.)

That means more than 99.9 percent of the time, customers land on pages that haven’t received a notice of potential counterfeit infringement, Fan said. Of course, that’s what the company has caught. But with 17.6 billion page views in October alone, according to web-analytics firm SimilarWeb, Amazon’s math suggests shoppers landed on about 17.6 million pages that hawked suspect goods that month. Amazon doesn’t release traffic data.

Amazon executives often trumpet the company’s investments to demonstrate how seriously it takes the matter. In a July filing to the Commerce Department, as part of its probe, Amazon’s vice president of public policy, Brian Huseman, noted the company spent $400 million in personnel costs last year to fight fraud and abuse, employing more than 5,000 workers.

Counterfeits are not just an Amazon problem. The Organization for Economic Cooperation and Development, a group of three dozen industrial countries, estimates counterfeit goods account for 3.3 percent of global trade.

But the problem is acute for Amazon, which has transformed itself into a dominant U.S. marketplace in part by opening its website to third-party merchants. By adding 2.5 million third-party sellers, the company has rapidly expanded its selection to more than 500 million items available, according to estimates by e-commerce research firm Marketplace Pulse. That adds massive selection, and the competition tends to drive prices down across the site, luring shoppers in the process.

Letting so many sellers in with few limitations has also created a marketplace for fakes that were more often found on street corners or flea markets. It’s easy for sellers to sign up for an account, and they can create listings for products, which Amazon scans with algorithms before they go live.

Allowing all those sellers has also opened a Pandora's box, making it impossible for Amazon to police the site's darkest corners to root out every scammer, said Juozas Kaziukėnas, chief executive of Marketplace Pulse.

"It will fundamentally never solve the problem because these issues are caused by scale," Kaziukėnas said.

Despite Amazon's algorithms designed to detect fakes, shoppers can type the phrase "YSL dupe" into the site's search bar and find knockoff handbags with Yves Saint Laurent's logo, as well as imitations of bags that use the logos and designs of such luxury brands as Louis Vuitton, Fendi and Gucci. A $10.97 knockoff Louis Vuitton passport holder recently carried the "Amazon's Choice" badge, a label the company uses to recommend products.

Plenty of customers are shopping for fakes on Amazon. Reviews left by consumers sometimes crow about the quality of a knockoff or how much less expensive it is than the real thing. Other times, consumers are duped, springing for products they assumed were authentic, only to get items that are sometimes poorly made or dangerous.

Lawmakers have stepped up criticism of tech giants, including Amazon, in recent months over their inability to control the massive platforms they run. Both Facebook and Twitter have been noted for their use in disinformation campaigns, while Amazon has been criticized for failing to police dangerous goods.

Many of the top luxury brands don't sell products directly to Amazon, so the online retailer counts on third-party merchants to stock and sell the items. Amazon has built out a global network of warehouses and incentivized third-party sellers to let it handle shipping to guarantee speedy Prime delivery. That also means that counterfeit goods are often brought onto its property, handled by warehouse workers and stocked on the company's shelves.

As Amazon has raced to add more and more selection, former executives say the company has come to accept that counterfeit items will find their way onto the site as well.

"Counterfeiting is a problem considered a necessary evil when you're going to be selling at this volume," said Chris McCabe, a former Amazon investigator who now consults for sellers on the site.

Brands have also sued Amazon. Daimler, the German automaker and parent company of Mercedes-Benz, accused Amazon of allowing the sale of fake Mercedes-Benz wheel caps in a November 2017 lawsuit. Amazon said the suit has been resolved, but declined to disclose details.

Birkenstock USA called out Amazon three years ago for trafficking in counterfeits and the sale of unauthorized products, after it quit selling its footwear directly to the retailer.

While it's still easy to find Birkenstocks, or products claiming to be made by the company, on the site, the complaints led Amazon to dial up efforts to remove fakes, according to the former Amazon retail executive.

The company launched a service called Brand Registry in 2017 that allows brands to register logos and intellectual property with Amazon so it can spot and remove listings when counterfeits are flagged. More than 200,000 brands have joined the program, Fan said. Amazon also beefed up staffing to address the issue.

Counterfeit complaints fell, but selection didn't grow as quickly as planned — so the company began adding more merchants, the former executive said.

Amazon's Fan disputed that account, saying the company has invested in protecting customers from its inception. "We continuously improve our protections and would never loosen them," Fan said.

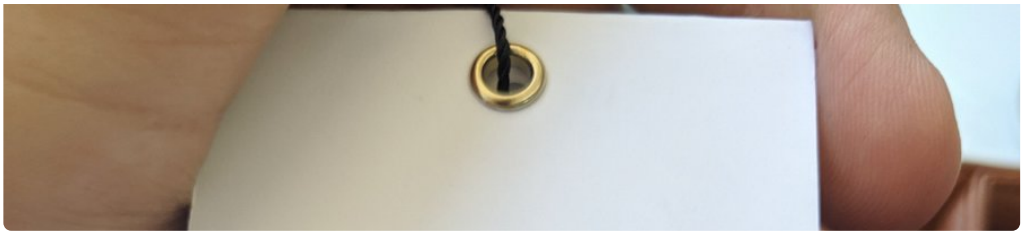
Fan said the company rooted out more than 1 million suspicious seller accounts last year before they started selling, and blocked more than 3 billion suspected bad listings.

Still, Philip Thomas recently bought a counterfeit Novel Duffle bag from Herschel Supply Co., which generally retails for $85. The New York-based tech executive didn't care much about color as he browsed, so he scrolled through the various options to pick a black version available for $45.10, even though it meant waiting three weeks for delivery.

The package arrived from China, and he quickly noticed shoddy stitching. Loose threads were hanging from the bag. But the real giveaway was a misspelling on a tag: "Limited Liferime Warranty."

Philip I. Thomas
@philipithomas

Just got my new @Herschelsupply bag from Amazon and . . . It's a clear counterfeit. Is this how you spell "Lifetime"?



6 2:44 PM - Jun 26, 2019

See Philip I. Thomas's other Tweets

After the seller failed to respond to Thomas, Amazon gave him a refund. But now the avid Amazon shopper said he's become skeptical about the authenticity of goods on the site. "It makes me more hesitant to trust the system to click 'Buy Now,'" Thomas said.

Cleaning up all the counterfeit goods on the site would require probing every claim of fraud, including those that show up in product reviews and shopper complaints. Brands also report both fakes and legitimate goods that they'd prefer not be sold on the site.

Rob Dunkel's Chicago-based data-analytics firm 3PM Solutions works with brands to spot counterfeits online. It first worked on a pilot project with Amazon to detect items that had a high probability of being fake, he said. But Amazon opted to end the pilot in 2017.

"We were willing to give it away to Amazon if it helped our customers and consumers," Dunkel said. "But because you are putting the information in front of them, they need to act."

Amazon's Fan said the company ended the project because it felt its technology was more advanced.

Luxury items like the Hermès bracelet are low-hanging fruit, frequently copied and easy to spot. Last month, The Post spent $164 on Amazon to pick up a handful of products that used logos and unique designs from brands such as Hermès, Gucci and Louis Vuitton to determine if they were fake.

Items included a $49.78 handbag that copied the iconic checkerboard design of Louis Vuitton's Neverfull bag that retails for $1,390, and a $29.90 belt with Gucci's double-G logo buckle, a vague replica of a belt the fashion brand sells for $450.

According to Kevin Ngo, a senior authenticator at The RealReal, an online consignment store that sells luxury goods, each item was a fraud. All of them were shipped via Prime in two days directly from Amazon's warehouses. Amazon has since taken down all those listings, Fan said.

Amazon's response to the counterfeit problem has been, in large measure, to ask brands to help it ferret out fakes. The company introduced an initiative in February that gives brands tools to remove listings of counterfeit products from Amazon's site.

“We do believe we can take counterfeits to zero, but we need brands to help do it because there are millions of brands,” Amazon’s retail chief Jeff Wilke said at a tech conference last month.

Amazon doesn’t publicly disclose the brands that participate in the program. But because luxury brands often don’t sell goods directly with Amazon, they are unlikely to participate. Louis Vuitton executives declined to comment for this article, but in written testimony to the Commerce Department, Anish Melwani, chief executive of LVMH Moet Hennessy Louis Vuitton’s North American operations, wrote it’s too costly and inefficient for retailers to police online marketplaces such as Amazon’s site for possible fakes. A person familiar with the business said Louis Vuitton does not participate in Amazon’s Brand Registry program.

Companies such as Louis Vuitton “can currently only ask for a reactive takedown of illicit listings, once the potential damage to the consumer has already been done,” Melwani wrote. And just as soon as one counterfeit item gets taken down, a product page for another emerges. Meanwhile, online retailers have “the necessary information and technical capabilities to efficiently and proactively detect, remove and prevent repeated infringements,” Malwani added.

That’s why some brands and trade groups are pushing to change liability laws that largely shield online retailers from financial responsibility of counterfeits. A change could incentivize Amazon and other online marketplaces to police their platforms.

“You should have some responsibility for that,” said Steve Lamar, executive vice president of the American Apparel & Footwear Association.

Amazon’s Huseman argued to maintain the status quo, suggesting in his testimony that shifting liability to online sellers would diminish the “immense opportunity to millions of honest entrepreneurs.”

But honest customers can get burned by counterfeits, too. Raul Noriega paid Amazon more than $1,000, a roughly 23 percent discount off the list price of $1,300, for a Tag Heuer Formula 1 watch in June, figuring he was getting a bargain. What he got, though, was a headache.

“I thought surely people who sell on Amazon are very reliable people who should have been vetted,” Noriega said. “It’s Amazon. It should be safe.”

The watch arrived at Noriega’s Johannesburg home with a warranty card that wasn’t dated or stamped. Suspicious, Noriega took the watch, which he purchased on Amazon’s U.S. site, to an authorized Tag Heuer dealer in town. He learned the watch was counterfeit because the numbers on the bezel were painted rather than engraved, the movement was tin-plated rather than gold-plated, and that the serial and model number engraving was the wrong size.

So Noriega reported it to South African police, which confiscated the watch as contraband. Even though authorities provided Noriega with a letter explaining the seizure, Amazon refused to initially refund his

purchase. The company gave Noriega his money back after being asked about the matter by The Post. Even after receiving his refund, Noriega said the ordeal has eroded his trust in Amazon.

“My opinion of Amazon has changed. I don’t see Amazon positively anymore,” Noriega said.

Jay Greene
Jay Greene is a reporter for The Washington Post who is focused on technology coverage in the Pacific Northwest. Follow

Get a year of access for $29. Cancel at any time.

Get this offer now

Already a subscriber? **Sign in**

EXHIBIT 5

By using this site, you agree to our **Privacy Policy** and our **Terms of Use**.

Watch TV

AMAZON · **Published** January 14

Amazon shoppers: Watch out for counterfeit versions of these 17 brand names

The tech giant has come under heavier scrutiny than other sites that work with third-party sellers for its counterfeit problem

Amazon is cracking down on counterfeit goods

FOX Business' Kristina Partsinevelos reports on how Amazon is addressing the problem of counterfeit sellers on their platform.

Amazon is expected to get more transparent about counterfeit products sold by third-party sellers on its platform, a person familiar with the company's initiative said.

Some luxury brands like Swatch have either backed out of plans to sell on Amazon or had no intention of selling goods on Amazon in the first place due to the tech giant's counterfeit problem, which has expanded in relation to an increase in third-party Chinese sellers on its platform as the company faces competition from the likes of Alibaba and eBay.

While eBay's counterfeit problem appears to be more serious, according to numbers compiled by The Counterfeit Report, Amazon is significantly more popular in terms of market size and its impact on the American public. The tech giant, therefore, has come under heavier scrutiny than other sites that work with third-party sellers for its counterfeit problem.

Steven Smith places packages onto a conveyor prior to Amazon robots transporting packages to chutes that are organized by zip code, at an Amazon warehouse facility in Goodyear, Ariz. (AP Photo/Ross D. Franklin)

"Our customers expect that when they make a purchase through Amazon's store — either directly from Amazon or from one of its millions of third-party sellers — they will receive authentic products," an Amazon spokesperson told FOX Business in a statement. "Amazon strictly prohibits the sale of counterfeit products and we invest heavily in both funds and company energy to ensure our policy is followed."

APPLE, MICHAEL KHORS AMONG WORLD'S MOST COUNTERFEITED BRANDS

"We investigate any claim of counterfeit thoroughly, including removing the item, permanently removing the bad actor, pursuing legal action or working with law enforcement as appropriate," the spokesperson said, adding that "over 99.9% of all Amazon page views by our customers landed on pages that did not receive a notice of potential counterfeit infringement."

Allbirds shoes

While the percentage of counterfeit items sold on Amazon is small, a study by review tracker Channel Signal notes that "a half percent of 200,000 reviews is 1,000 reviews about fake product that consumers are reading," which is still a huge number that puts sellers and consumers at risk. Examples of brands that have been subject to counterfeit sellers include:

1. Apple
2. Nike
3. Adidas
4. Hermes
5. Allbirds
6. Birkenstocks
7. Ray-Bans
8. Sharpie
9. BMW
10. Gillette
11. Canada Goose

12. Hydro Flask
13. Vans
14. Yeti
15. Urban Decay
16. Under Armor
17. Sony

A number of other fake name-brand items can be seen on The Counterfeit Report.

Automotive company Daimler AG, which owns Mercedes, sued Amazon directly for selling counterfeit auto parts in October 2017. Williams-Sanoma sued the tech giant in 2018 for selling a furniture line with products that were "strikingly similar" to Williams-Sonoma's West Elm brand. A number of families and companies have sued Amazon for selling problematic hoverboards that have caused an estimated $2.3 million in damage, according to a December report.

FTC TO CRACK DOWN ON FAKE AMAZON REVIEWS

That's why Amazon has been holding meetings with government officials in recent weeks to tackle the problem, the source familiar with the program told Reuters in a report published Monday.

A festivalgoer wears Canada Goose while riding the ski lift at Canyons during the 2018 Sundance Film Festival on Jan. 22, 2018, in Park City, Utah. (Rich Fury/Getty Images for Canada Goose)

The tech giant launched Project Zero in the U.S. in February 2019 in an effort to identify counterfeit products and stop the sellers from profiting off sales of goods with fake labels instead of leaving consumers to the task.

"Project Zero ... empowers brands to help us drive counterfeit to zero by combining Amazon's machine learning technology with the unique knowledge brands have of their own intellectual property," Amazon told FOX Business in a statement. "Using the self-

service counterfeit removal tool in Project Zero, brands can instantly remove counterfeit from our store and this information is fed into our automated protections so we can more effectively prevent counterfeit listings in the future."

CLICK HERE TO GET THE FOX BUSINESS APP

Amazon also launched its Intellectual Property (IP) Accelerator program in October, which offers sellers an efficient way to obtain IP rights and brand protection. Additionally, the company started another program to combat counterfeit products called the Utility Patent Neutral Evaluation Process, which will connect two sellers offering the same products -- one patented and one counterfeit -- and a third-party lawyer to solve the issue.

Workers walk past boxes to be shipped inside of an Amazon fulfillment center in Robbinsville, New Jersey, Nov. 27, 2017. (REUTERS/Lucas Jackson)

Additionally, Amazon's Transparency program "is an item-level tracing service where brands serialize each unit they manufacture with a unique code. Amazon then scans these codes and verifies the authenticity of the product before it reaches a customer. Customers can also scan the Transparency code via a mobile app to confirm authenticity and learn more about the product, such as usage instructions, ingredients, and expiration date," a spokesperson said in a statement.

A number of brands including Nite Ize, Vera Bradley and Otterbox have also partnered with Amazon in successful lawsuits against sellers that sell counterfeit products.

CLICK HERE TO READ MORE ON FOX BUSINESS

To identify fake products, look out for prices that seem too low (for example, a pair of real Adidas sneakers likely won't sell for $20) and compare prices on Amazon to prices on brand websites; look at the name of the seller; and read reviews from other customers. Be skeptical of requests from a third-party seller to contact them before

purchase, blurry or small photos of the product and sellers trying to convince consumers to click on a link outside Amazon.

Quotes delayed at least 15 minutes. Real-time quotes provided by BATS BZX Real-Time Price. Market Data provided by Interactive Data (Terms & Conditions). Powered and Implemented by Interactive Data Managed Solutions. Company fundamental data provided by Morningstar. Earnings estimates data provided by Zacks. Mutual fund and ETF data provided by Lipper. Economic data provided by Econoday. Dow Jones & Company Terms & Conditions.

This material may not be published, broadcast, rewritten, or redistributed. ©2020 FOX News Network, LLC. All rights reserved. FAQ - Updated Privacy Policy

EXHIBIT 6

CNN
LIVE TV

Fake and dangerous kids products are turning up for sale on Amazon

By Pamela Boykoff and Clare Sebastian, CNN Business

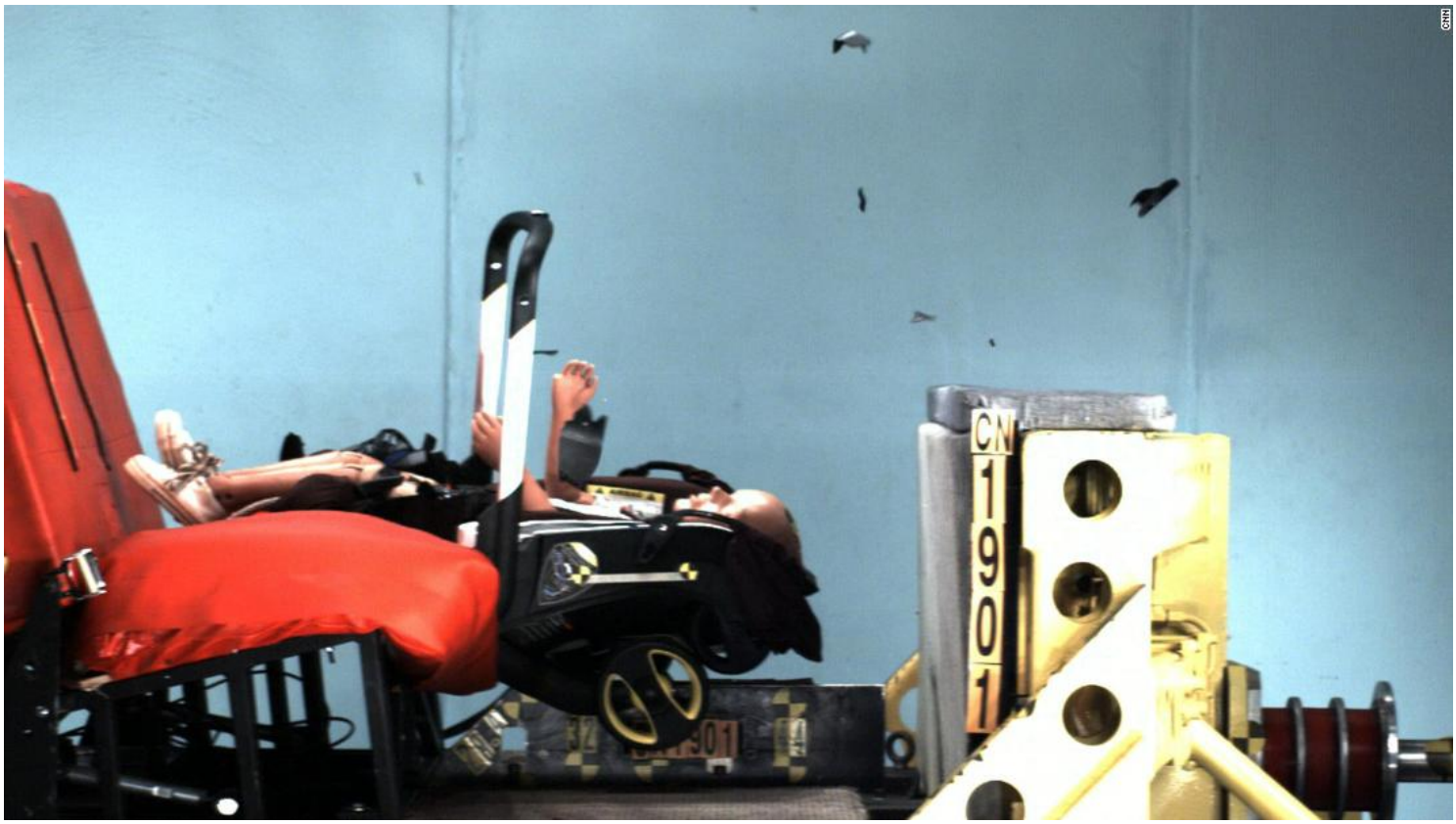
Updated 8:25 AM ET, Mon December 23, 2019

New York (CNN Business) — The listing on Amazon (AMZN) described it as a "4 in 1 Baby car seat and Stroller" and featured images of a popular brand called Doona, including a photo of the US President's daughter, Ivanka Trump, with hers. Listed for $299, this copycat was $200 cheaper than a real Doona. It was also potentially dangerous for children.

The car seat broke into pieces in a 30 mph crash test commissioned by CNN, failing to meet the basic standards set by US regulators. Video of the test shows the toddler dummy twisting as the car seat fractures and slides forward, with plastic pieces that have broken off it flying through the air. In an identical crash test scenario, an authentic Doona met federal requirements, with the car seat remaining in one piece and in place around the dummy.

Dr. Alisa Baer, a pediatrician and nationally certified child passenger safety instructor, reviewed the test results and said in a real crash such a car seat failure could put a child in "grave danger," and lead to injuries to a child's chest, neck or head, including a traumatic brain injury.

on Amazon. Seven different business owners told CNN their products were being actively targeted by counterfeiters using Amazon's marketplace for third-party vendors. The businesses said Amazon put the onus on them to report suspicious listings and that this often amounted to a game of "whack-a-mole," in which new listings appeared almost as soon as flagged ones were taken down.



A car seat purchased on Amazon fractured in a 30 mph crash test, failing to meet federal standards

Under current US case law, Amazon is not liable when third-party products sold on its site directly infringe on intellectual property or have safety defects. The liability lies with the third-party seller. This is fundamentally different from how the law treats brick-and-mortar retailers like Target (TGT) or Walmart (WMT) or even your corner grocery. If you find a product at a physical store that infringes on your trademark, or you buy something defective there, you can sue the store even though they didn't make the product.

WORK TRANSFORMED

Work Transformed is your guide to navigating this new normal. Sign up for tips and tactics from CNN Business.

Sign Me Up

No, Thanks

By subscribing you agree to our privacy policy.

ecommerce platform and its dominance is growing. According to an estimate from data firm eMarketer, Amazon controls 37.7% of US ecommerce sales and that share is expected to grow. Many of the brands that spoke to CNN told us they can't afford not to sell their products on Amazon. As an Amazon spokesperson said to CNN in a statement, "our customers expect that when they make a purchase through Amazon's store—either directly from Amazon or from one of its millions of third-party sellers—they will receive authentic products."

Amiad Raviv, the commercial manager of Doona, said the company has found more than 40 Amazon listings this year that contained fake versions of its products or versions that infringed on its intellectual property. Doona flags the listings they are concerned about to Amazon, which then removes them. According to Raviv and the other business owners CNN spoke with, this piecemeal process means listings are often online for several days, leading to a significant window when consumers can buy the potentially dangerous product.

The imitation Doonas are sold through Amazon's website or app, but not by Amazon directly. According to Amazon's 2018 annual report, 58% of Amazon's sales came from its millions of third-party sellers, many of whom ship directly to consumers. Many legitimate brands, including Doona, sell products through authorized third parties. However, items purchased this way may never be checked by Amazon employees or pass through an Amazon warehouse.

"A lot of people on the Amazon platform think that because it's on Amazon, it is a genuine product. And that's actually really not the case," said Raviv.

The product CNN bought was listed by a seller called Strolex and shipped from China. All US car seats are required to be certified according to NHTSA standards, but this seat did not have any US certification labels. On the Amazon listing, it claimed to have European certification, but when it arrived it was missing a required European certification label and the European registration number in the instruction manual was a copy of Doona's.

Baer examined the car seat before the crash test and pointed out several things she saw as red flags. The word "always" was misspelled "aiways" on the anti-rebound bar, the seat featured European warning labels instead of

The Strolex listing disappeared from Amazon shortly after CNN ordered the seat, but the seller Strolex remained on the site though with no active listings. When reached by phone in China, a representative of Strolex said in English "my products are safe," but refused to give his name or answer any other questions.

The results of the crash test were sent by CNN to Amazon for review. A week later, Amazon sent an email to customers who bought the product, warning them of a safety issue and saying it "may not be a genuine product." The email urged customers to stop using the product immediately and offered a full refund.

Amazon told CNN safety was a top priority, but also that sellers are responsible for meeting Amazon's "high bar" for the quality of products. "We require all products offered in our store to comply with applicable laws and regulations and have developed industry-leading tools to prevent unsafe or non-compliant products from being listed in our stores," an Amazon spokesperson said in an emailed statement.

Not just car seats

Luanne Whiting-Lager and Bengt Lager first realized their "Love to Dream" baby swaddle was being copied last year when a customer called to complain that a zipper pull had broken off the swaddle, frightening the new mom and creating a potential choking hazard for her baby. The customer thought she had purchased a real version of the $34.99 swaddle through Amazon's marketplace, but the couple's company, Regal Lager, examined it and realized it was a counterfeit. The fake product used the Love to Dream trademark and also copied the brand's patented swaddle shape, which allows the baby to bring their hands to their mouth while swaddled. Regal Lager provided CNN a photo of the fake swaddle and the original invoice.

Regal Lager is the exclusive distributor for the "Love to Dream" swaddle in the United States and participates in the Amazon Brand Registry, Amazon's official program to help businesses protect their intellectual property.

The company found complaints online about the fake product's zippers falling off and the product's neck opening being too large or small, another potential safety problem since it can ride up over the baby's mouth while it sleeps or be too restrictive around the neck.

The real "Love to Dream" swaddle

Eventually, the company hired an agency, Marketplace Ninjas, which helps brands operating on Amazon and the two convinced Amazon to take down 20 different listings for infringing upon versions of their product. The agency monitors Amazon and other e-commerce site all the time, watching as the counterfeiters employ new tactics to get past safeguards, like listing the product as Luv 2 Dream initially and then changing it to match their trademark Love to Dream. "One taken down, another pops up," Whiting-Lager said.

Regal Lager says the cheaper copycats have had a negative impact on their business. They estimated they've lost about $250,000 in the whole ordeal or about 3% of their Amazon sales, based on their sales volum

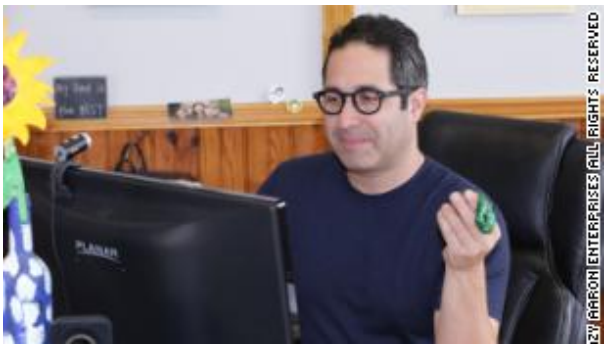
The couple like working with Amazon, but think the company needs to take full responsibility for the products on the platform and could take steps to restrict who can post products using Amazon's specific identification numbers to control counterfeits.

"The whack-a-mole game"

Amazon offers three programs designed to help companies protect their brand from counterfeits. While business owners CNN spoke to say Amazon's initiatives have helped tackle the problem, they complain the responsibility — and cost — of policing fakes feels like it falls on them rather than on Amazon.

The company said more than 200,000 companies participate in the Amazon Brand Registry. This program started in 2017, is free and gives rights owners tools to help manage and protect their brands, including the ability to search their global listing by word or image and flag potential infringers. Amazon also automatically scans its site to proactively remove suspicious listings. According to Amazon, "brands in Brand Registry on average are finding and reporting 99% fewer suspected infringements than before the launch of Brand Registry."

Aaron Muderick, the founder of Crazy Aaron's Thinking Putty, said his receptionist spends 15 to 20 hours a week submitting forms asking Amazon and other ecommerce sites to remove products that use his company's



Aaron Muderick, founder of Crazy Aaron's Thinking Putty.

He participates in the Amazon Brand Registry. He says the tool is useful and has improved over time, but he finds it disappointing given Amazon's reputation for AI and software prowess.

"It doesn't work as well as I would expect," Muderick said. "While the whack-a-mole game has gotten a little bit better, it still exists every single day."

Charlotte Wenham, the Executive Officer of pNeo, also participated in Amazon's brand registry when she discovered in 2018 that sophisticated counterfeiters were targeting her company's Baby Shusher, a sound machine designed to help babies sleep. Based the seller complaints, Wenham believed there was a real risk of harm should the battery fluid leak from a counterfeit product onto a sleeping baby.

Wenham said the counterfeit products used Baby Shusher's branding and replicated the real product's packaging and user manual. Iris Wilbur-Kamien thought she had bought a genuine Baby Shusher on Amazon until it fell apart just five months after she purchased it. Only when the real company asked her to send a photo of the product's identification code did she realize it was a counterfeit, she told CNN. There wasn't one.

Wenham said the impact on her business from the flood of counterfeits was significant, costing more than $100,000 by her estimate. She believes in cases where a genuine manufacturer is being besieged by counterfeits, Amazon should move a lot faster. Every day the counterfeits remained on the site, she said, was a day she lost sales.

A counterfeit Baby Shusher product (left) next to the genuine article (right).

countries.

Amazon also provides a service called Transparency, where brands can add unique codes to products. These codes can be scanned by Amazon and by customers to confirm authenticity, but brands have to buy the special labels from Amazon at a cost of from 1-5 cents per item. The brands also have pay to add the labels to each product. Amazon said over 6,000 brands have enrolled in Transparency.

Regal Lager declined to participate in Transparency, primarily because of the costs involved. "It's like the good guys are having to pay for the bad guys' behavior and it just seems backwards," Bengt Lager said.

Signs of a potential counterfeit

1. Check the seller. If you have any doubts, ask the manufacturer for a list of authorized distributors.
2. Look for misspellings or poor grammar in the listing.
3. Consider the price. If it's much lower than the competition, it could be fake.
4. Shipping time. Anything more than two weeks could be a red flag.

Recently, Amazon added a third brand protection service called Project Zero, which uses the ecommerce giant's machine learning technology. Amazon describes the program as giving brands access to a "self-service counterfeit removal tool" that allows them to instantly remove counterfeits from the platform while also providing feedback into Amazon's automated system to identify fakes.

At his headquarters in Norristown, Pennsylvania, Aaron Muderick keeps a wall of shame showing copycat products. Children's putty may not sound like a risky product, but European regulators have issued 19 separate safety alerts for putty and slime products in the last year, ordering sales bans or recalls because of high levels of boron, lead and barium and potentially dangerous magnets.

As Muderick has become more aggressive about flagging trademark violations, he sees the competing products reappear under new names and packaging. These generic product names do not violate his trademarks, but he continues to be concerned about their safety. He estimated the infringing and copycat products cost him 10-30% of his sales.

CNN purchased a six-pack of generic magnetic putty on Amazon. Each tin of the product included putty and a small magnet that could be used to attract or repel it. Testing found the magnets included in the set did not meet federal standards for toys intended for children under 14. The product listing on Amazon was labelled as suitable for children ages 3 and up. Magnets that are both small and powerful are not permitted in children's toys because of the risk a child could swallow a magnet and metal item, leading to an intestinal blockage or perforation. Researchers affiliated with Rutgers University tested the magnet for CNN and found it was substantially stronger than the federal limit for a magnet that is small enough to be swallowed.

Muderick said he's frequently found generic putty products that he believes are unsafe, but it's not clear to him how to alert Amazon to his concerns. While Amazon is responsive when he submits a form saying a listing violates his copyrights and trademarks, he said the process is much more opaque when it comes to reporting suspected safety issues.

Amazon said they are investigating counterfeits associated with the brands included in CNN's reporting and will take "appropriate action against the sellers involved." An Amazon spokesperson described the various issues these businesses reported to CNN as "isolated incidents that do not reflect the fantastic products and customer experience provided by millions of small businesses selling in our store."

"I am sort of just mystified"

uphold the notion that liability doesn't apply to ecommerce sites in the same way as a physical store. When it comes to third-party sales, ecommerce sites argue they are just a platform providing a virtual meeting place for buyers and sellers to interact. Amazon has also argued that it is protected by section 230 of the Communications Decency Act, a federal law that protects online sites from liability for speech by others on their platforms, because the company believes it covers the claims and the warnings made in product listings.

Now, some courts are beginning to question whether it's time to rethink past decisions on Amazon's liability, given the company's extensive control over its marketplace and the difficulties involved for consumers trying to sue third-party sellers.

A Philadelphia appeals court recently ruled Amazon could be held liable in the case of a woman who was blinded in one eye when a defective dog collar she had purchased from Amazon broke and a retractable dog leash attached to it hit her. Neither she nor Amazon could locate the third-party company from which she had bought the collar. In their decision, the judges in the case concluded, among other things, that Amazon exerts "substantial control" over its vendors and was the only party available to the injured plaintiff for redress.

Sadie the dog. When a defective collar purchased from Amazon that Sadie was wearing broke, a retractable leash attached to it snapped back and hit her owner, blinding her in one eye.

Amazon had argued that it was not the seller in this case, but a marketplace provider, and thus not subject to the liability claims. It also argues it was protected the claims were barred by the Communications Decency Act.

Given the significance of the decision, the entire Third Circuit Court of Appeals has agreed to review the decision in 2020. The initial decision has no legal effect pending that review.

Mark Geistfeld, a professor at the NYU School of Law who specializes in product liability, said he believes it's just a matter of time until legal interpretations begin to change regarding Amazon's liabilities. He said the key issue is consumer expectations. A shopper in a physical store or on Amazon understands something could be manufactured by a third party, but, with both purchases, they are expecting the product is not defective or counterfeit.

Also at issue is the amount of control Amazon exerts over its site, in terms of how listings are presented to customers, the terms it makes sellers sign and the level of information available using artificial intelligence software. Trademark cases such as Tiffany v. eBay, which set out in 2010 that ecommerce platforms were not responsible for infringing sellers, now look out of date to some lawyers.

"Something is shifting. It can't be the same standard that was used 10 years ago," said Kari Kammel, from the Center for Anti-Counterfeiting and Product Protection at Michigan State University.

Jason Drangel, a lawyer who represents several major toy manufacturers in counterfeiting lawsuits, agrees.

"The platforms that exist now basically control the products, they understand that the products come from a specific country, a specific seller located in China," he said. "It's a different world and that's part of the problem."

Politicians are also beginning to pile on the pressure over counterfeits and safety in the Amazon marketplace.

In August, three Democratic senators wrote a letter to Amazon CEO Jeff Bezos, expressing their "grave concerns regarding Amazon's failure to remove illegal, deadly and deceptive products, and to provide visible warnings on the products sold on your platform." The letter was in response to a Wall Street Journal investigation into counterfeits on the site. Senators Richard Blumenthal, Robert Menendez and Edward Markey included a list of questions for Bezos about how he will ensure safety on the platform. Senator Menendez's office told CNN the response from Amazon didn't adequately address their concerns.

At a July House hearing on counterfeits, Republican Congressman Doug Collins questioned why representatives of Amazon, eBay (EBAY) and Walmart failed to attend. He urged platforms to find a more effective, automated process for detecting and blocking counterfeit listings, to create better ways to vet sellers and prevent counterfeiters from listing products again and again under different names, and to stop counterfeiters from using genuine photos of brands to market their products without their consent.

"These solutions are well within the grasp of our large online marketplaces and practices they should have already implemented on their own," Rep. Collins said.

Amazon did not provide CNN with a direct response to either the letter from the senators or Representative Collins' comments, but did tell CNN that in 2018, its teams used a mixture of proprietary technology and manual reviewers to proactively block more than three billion suspect listings for various forms of abuse, including non-compliance, before they appeared in the store.

Muderick from Crazy Aaron's thinks a legislative change may be the only way to end the game brands like his are playing against the fake listings of infringing and potentially dangerous products.

"I think unless someone is liable, nothing is going to get better," he said.

Kelly Burns, Jacqueline Davalos and Winston Lo contributed reporting.

Update: This story has been updated to clarify Amazon's comments to legislators.

FOLLOW CNN BUSINESS

Most stock quote data provided by BATS. Market indices are shown in real time, except for the DJIA, which is delayed by two minutes. All times are ET. Disclaimer. Morningstar: Copyright 2018 Morningstar, Inc. All Rights Reserved. Factset: FactSet Research Systems Inc.2018. All rights reserved. Chicago Mercantile Association: Certain market data is the property of Chicago Mercantile Exchange Inc. and its licensors. All rights reserved. Dow Jones: The Dow Jones branded indices are proprietary to and are calculated, distributed and marketed by DJI Opco, a subsidiary of S&P Dow

LIVE TV

Jones Trademark Holdings LLC. All content of the Dow Jones branded indices Copyright S&P Dow Jones Indices LLC 2018 and/or its affiliates.

Terms of Use Privacy Policy Do Not Sell My Personal Information AdChoices About Us CNN Studio Tours

CNN Store Newsletters Transcripts License Footage CNN Newsource Sitemap

© 2020 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.
CNN Sans ™ & © 2016 Cable News Network.

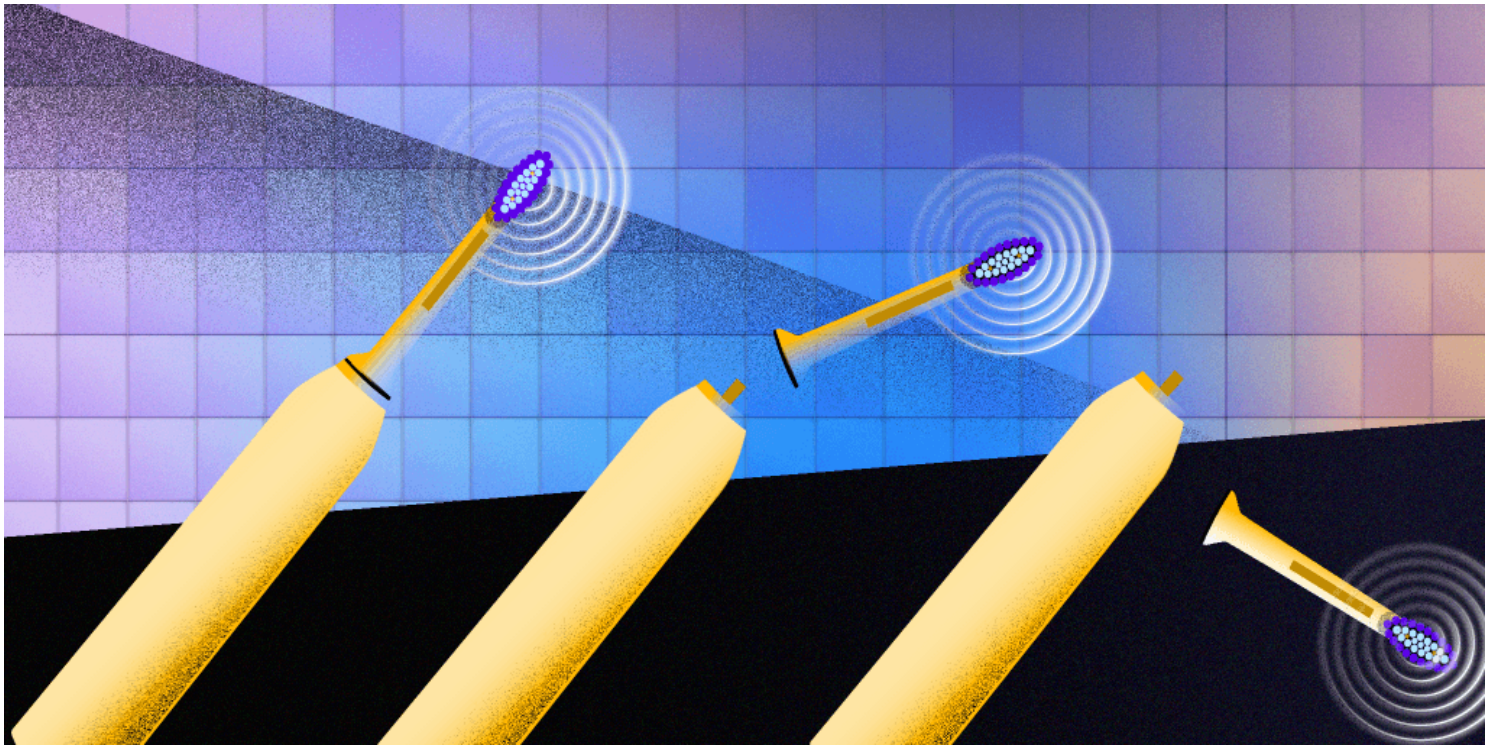
EXHIBIT 7

wirecutter
A New York Times Company

Wirecutter is reader-supported. When you buy through links on our site, we may earn an affiliate commission. Learn more

Real Talk

Advice, staff picks, mythbusting, and more. Let us help you.



Ilustration: Sarah MacReading

Welcome to the Era of Fake Products

PUBLISHED FEBRUARY 11, 2020

Ganda Suthivarakom

Imagine walking into your local grocery store and seeing two virtually identical cartons of milk right next to each other. The only discernible

difference—and it's barely discernible—is that there's a tiny tag on one carton saying the milk is sold by a third-party seller. Oh, and it might have rat poop in it.

This scenario isn't all that far from what's happening in e-commerce retailers' massive, hard-to-police markets of third-party sellers.

The rise of counterfeit goods and other phony products sold on the Internet has been swift—and it has largely gone unnoticed by many shoppers. But make no mistake: The problem is extensive. Most people don't realize this, but the majority of listings on Amazon aren't actually for items sold by Amazon—they're run by third-party sellers. And even though many, many third-party sellers are upstanding merchants, an awful lot of them are peddling fakes.

A major Wall Street Journal investigation recently revealed that Amazon has listed "thousands of banned, unsafe, or mislabeled products," from dangerous children's products to electronics with fake certifications. The Verge reported that even Amazon's listings for its own line of goods are "getting hijacked by impostor sellers." CNBC found that Amazon has shipped expired foods—including baby formula—to customers, pointing to an inability to monitor something as basic as an expiration date. Because of the proliferation of counterfeits and what Birkenstock describes as Amazon's unwillingness to help it fight them, Birkenstock won't sell on Amazon anymore. Nike announced that it is also pulling out of Amazon. "Many consumers are … unaware of the significant probabilities they face of being defrauded by counterfeiters when they shop on e-commerce platforms," reads a January 2020 Department of Homeland Security report (PDF) recommending measures that would force e-retailers to take counterfeits even more seriously. "These probabilities are unacceptably high and appear to be rising."

This is something we care a lot about here at Wirecutter. After all, we're in the business of recommending the best products to our readers. We want to make sure that if you act on our advice, you actually get the top-quality product we're recommending and not some third-rate knockoff.

Over several months of research, we were able to purchase items through Amazon Prime that were either confirmed counterfeits, lookalikes unsafe for use, or otherwise misrepresented. We talked with many brands about the rise of fakery and their efforts to combat it. And we tried to

understand the new landscape of counterfeits and how to navigate it, so that you can as well.

Amazon, too, is clearly aware of the problem and is taking plenty of measures to combat counterfeits on its site. But critics say its efforts are not nearly enough. (Read more about Amazon's efforts to fight counterfeits here.)

In the 2010s, the spread of misinformation and "fake news" meant learning to consume articles and news programs with skepticism. In this decade, as e-commerce sites increasingly become our go-to for nearly every purchase we make, the proliferation of fake products—and fake reviews—will similarly train a generation of consumers to be skeptical and careful about what they buy.

Welcome to the era of fake products.

Burned by fake gloves

The real 'Ove' Glove and the fake 'Ove' Glove look nearly identical. Photo: Ganda Suthivarakom

"Sometimes, removing pans from the oven can be too hot to handle—ouch!" warns the cheesy voiceover on late-night commercials for the 'Ove' Glove. The heat-proof glove, made of meta-aramid fibers and cotton, with strips of silicone that can withstand temps of 540 degrees Fahrenheit, made its name in the early 2010s with funny, easy-to-mock ads. But the 'Ove' Glove had plenty going for it—an endorsement by Consumer

Reports, the Good Housekeeping Seal, and on and on. It was a highly unique product, and the company took steps to protect itself with a design patent (D567,454) and a trademark.

Despite those efforts, the small, San Francisco–based company has had to contend with counterfeit sellers on its own product pages on Amazon and other sites.

"JOSEPH ENTERPRISES INC (Joseph Ent): is the only legal manufacturer and distributor of the trademarked 'Ove' Glove," the product page states clearly. However, I was able to purchase a fake 'Ove' Glove through Amazon Prime from a seller named Winifred Connor, who has since been removed from the store.

Michael Hirsch, vice president of Joseph Enterprises, told us that the process of getting fraudulent third-party sellers removed can take months and involves painstakingly buying suspected fakes and documenting the problem for Amazon. Though the exact rules of the algorithm are not public knowledge, counterfeiters likely "win the buy box" (or become the seller that gets to fulfill an order) by posting the lowest prices, so alternate sellers get to fulfill orders for customers instead of Joseph Enterprises. We bought our fake for $9.86 on Amazon, about $5 less than the price Joseph Enterprises set. We were even able to find obvious fakes selling for $2 apiece in bulk on Chinese commerce site Alibaba.

Because there are rarely consequences for selling fakes, beyond a seller disappearing from a site, the seller can just reestablish its presence to continue to move its inventory. "Once they're off, they come back under a different brand and name," Hirsch said. He laments not just the loss of customers but the danger posed by fakes. "Customers have literally been burned by using an inferior product," he said. Given this and other problems the company has encountered, Hirsch said he recommends that customers buy the 'Ove' Glove from Target's site or at brick-and-mortar retailers.

We reached out to Amazon about the fake 'Ove' Gloves and the problematic seller. The seller was removed from the site shortly after we purchased the fake glove.

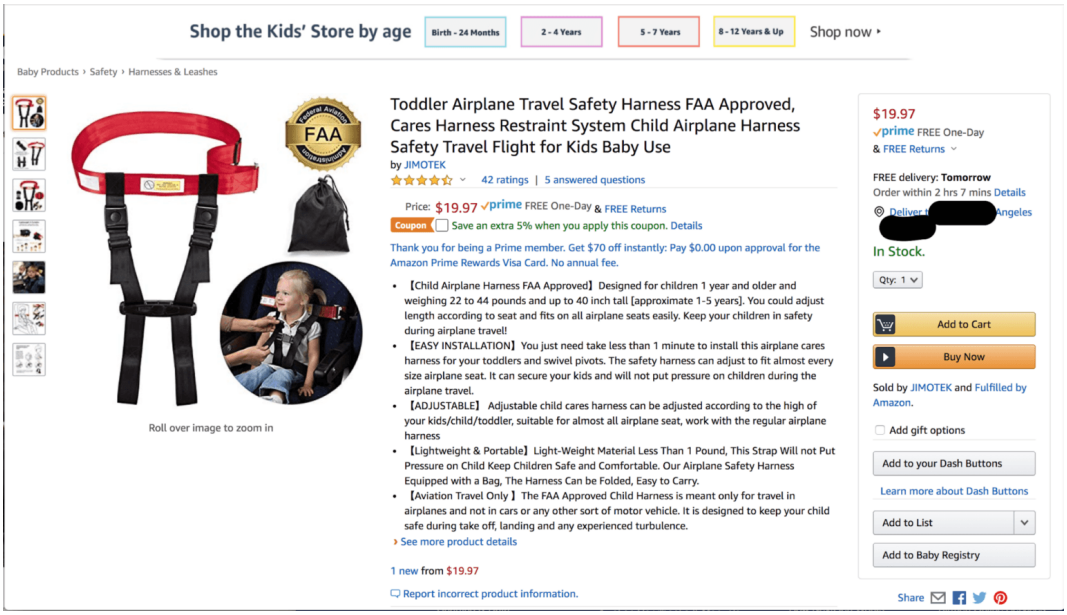
Fakes for kids

Wirecutter recommends the authentic Kids Fly Safe CARES Airplane Safety Harness for people who want to secure smaller children on planes without having to lug a heavy car seat. The patented and trademarked harness is made by AmSafe, an aviation manufacturer that specializes in building restraint systems for commercial aircraft. As a Federal Aviation Administration representative told us, "The AmSafe product called CARES (Child Aviation Restraint System) was certified as an ELOS—Equivalent Level of Safety—to a car seat. It is the only harness type child safety restraint that the FAA has certified (PDF)."

But I was able to purchase a copycat "Toddler Airplane Travel Safety Harness" with a label that fraudulently claimed it was "FAA approved." The materials were inferior to those of the real CARES harness, with cheap plastic buckles, weak stitching, and no lock to keep the adjustable shoulder straps in place.

AmSafe told us that it has put hundreds of thousands of dollars into testing the safety of its product, running more than 100 sled tests with crash test dummies to simulate flight conditions. Knockoff manufacturers sew nylon straps together to create a $20 product that may look like the Kids Fly Safe CARES harness, but "it's all in the sewing and the webbing," said Charley Fussner, business unit director of seatbelts at AmSafe. Although there are currently six sellers for the CARES harness, the only authorized seller on Amazon is River Colony Trading, Fussner said.

We reached out to Amazon and the FAA about this knockoff. Shortly after I contacted the FAA, the product was removed from Amazon. However, another harness listing has popped up under a different name, using the same imagery (minus the FAA label), and with a price of $50 instead of $20.



This Amazon listing for a counterfeit CARES airplane restraint harness falsely claimed that the copycat was FAA approved. It was selling for about $50 less than an authentic CARES harness and looks nearly identical, at least in the listing.

As The Washington Post and CNN have recently reported, kids car seats and strollers have also been copied and knocked off by counterfeiters. Amazon relies on third-party sellers to self-certify that a product complies with all safety laws. But as Inc. has reported, Amazon isn't reviewing safety documentation before a product gets posted to the site by third-party sellers, allowing unsafe car seats to slip through.

Jon Sumroy is the inventor of the Mifold travel booster, a patented, Indiegogo-born car seat that folds up smaller than an iPad for easy transport from one car to another. He says he began to see copycats almost as soon as he launched his company: "They don't copy exactly the design, but what they have done is copy the concept of the product."

We were able to purchase the YXTDZ portable and foldable child booster seat, a cheap plastic seat similar to the Mifold, but with none of the reinforced metal or safety labels required by law for children's car booster seats. The listing has since been removed. The fake is worrying—it looks about as sturdy as a flimsy toy you might buy at a swap meet. We reached out to the seller to request safety information but did not get a reply.

The YXTDZ is a cheap copy of a car booster seat called the Mifold, but without the safety labeling or documentation that it meets federal standards.

Copies like the YXTDZ lack the clear labeling and safety test results of the compliant Mifold (Sumroy compares his invention to cheap knockoffs in this video). The physical distinctions between the products are clear, but the invisible differences are far more worrisome. And because Sumroy is faced with a knockoff rather than a counterfeit, Amazon's anti-counterfeiting tools can't be used to combat the problem.

We reached out to Amazon about this product. The YXTDZ storefront still exists, but it is no longer offering the car booster seat on Amazon.

The third-party seller system: a boon to counterfeiters

Counterfeits have always been an issue. But the Internet has exacerbated the problem.

In the brick-and-mortar days, a counterfeit product might have a harder time getting onto the shelves of a legitimate business, since it would be in a retailer's best interest to vet the validity and safety of products the retailer might be liable for selling to a customer. Business owners were gatekeepers, and counterfeits were largely relegated to back alleys, figuratively and literally.

Things are different online. Smaller vendors who peddle counterfeits, particularly pseudonymous third-party sellers on e-commerce platforms with broad reach and trust, now have access to millions of customers they never had when they were lurking in downtown alleys and flea markets. "The rise of e-commerce has led to the rise in counterfeits," says Kim

Gianopoulos, director of a Government Accountability Office (GAO) team that investigated counterfeits for sale online.

If you shop on Amazon, you've probably bought things from third-party sellers without knowing it. I have. Third-party sellers now dominate Amazon sales, accounting for 54 percent of units sold on Amazon in the second quarter of 2019, according to Statista. "Third-party sellers are kicking our first-party butt," Amazon CEO Jeff Bezos told shareholders in a 2019 letter, calling the increase—from 3 percent of sales in 2000 to over half today—"remarkable." Annual third-party sales have grown to a whopping $160 billion.

> **You've probably bought things from third-party sellers without knowing it. I have.**

Making things particularly tricky is the fact that a single e-commerce product page may include offerings from the manufacturer as well as from many third-party sellers, some honest and some not so honest. On an e-commerce site, it's as though those back-alley and swap-meet sellers have gotten to put their wares inside the store, on the same shelf as the real goods. And product placement relies on an algorithm that can push the cheapest version to the front of the shelf.

This would be fine if all third-party sellers were committed to honest sales of authentic goods. And it's important to note again that many third-party sellers are upstanding. But with so many sellers competing for clicks, one way to win the customer is by offering the lowest price, and it's often easier to bring the price down if you're selling a counterfeit.

At Wirecutter, we've seen this problem pop up with fake tweezers and bogus umbrellas. Counterfeiters have infiltrated categories as niche as bird feeders and cleaning devices. You don't even have to manufacture a fake to sell them—just do a search for Kylie Cosmetics or Hydroflask on Alibaba to see barely concealed counterfeits that can be bought in bulk for a fraction of the street price.

These are clear fakes for sale on Alibaba. The lip-gloss box doesn't say Kylie, but everything else is an exact match to her company's packaging.

These are clear fakes for sale on Alibaba. The Hydro Flask logo shown here is using the wrong font.

Angry customers who confuse fakes for the real thing can have a devastating effect on public perception of a brand. For instance, the maker of Brush Hero, a hose attachment for cleaning, saw the listing for his product get undercut by sellers offering a much lower price for poor-quality counterfeits, Inc. reported. In November, The Wall Street Journal reported that Brush Hero's business could not withstand the effect of counterfeits and would be laying off most of its US staff.

"What's sad besides consumers being ripped off is that honest sellers, people that work their butts off, are being ripped off too," says Rob Gross, co-founder and COO of Fakespot, a website that analyzes the veracity of

customer reviews on e-commerce product pages. “They’re being ripped off by the competitors, and they’re being ripped off by Amazon, because Amazon’s not doing enough to protect real, honest sellers.”

Complaints about fakes are on the rise

The sale of counterfeit items now represents 3.3 percent of world trade, according to the Organisation for Economic Co-operation and Development, an international group with 36 member countries (including the US) that provides analysis and policy recommendations. The value of seized goods in the US (if they’d been real) was almost $1.4 billion in 2018, according to US Customs and Border Protection. Worldwide, there have been instances of fake chargers causing electrocution deaths (PDF), phony cosmetics making a buyer’s face swell up, and pet supplements sickening dogs. Immigration and Customs Enforcement and other law enforcement agencies have reported finding carcinogens, bacteria, and waste from both humans and rodents in counterfeit cosmetics. Fake chargers and cheaply-made lithium ion batteries can damage your electronics and even catch fire.

A 2018 GAO report on counterfeits recounts that of 47 products agency employees purchased from third-party sellers with good ratings, 20 were fake, as confirmed by the intellectual property rights holders. One hundred percent of Nike Air Jordans were real. One hundred percent of Urban Decay eye primer makeup tubes were fake.

This review doesn't say "fake" or "counterfeit," but that's certainly the gist of it.

1 of 2

I asked Tommy Noonan, founder of ReviewMeta, a site that evaluates the quality of the reviews on Amazon product pages, if he would run an analysis of all reviews ReviewMeta had collected that were posted to Amazon from January 2015 through October 2019. Noonan found that products with reviews mentioning the keyword "counterfeit," "counterfiet," or "fake" were on the rise, accounting for 1.725 percent of reviews in 2015 and 4.275 percent in 2019.

"It's impossible for me (or anyone else) to accurately determine which products are counterfeit on Amazon and which aren't," Noonan emphasizes. And his analysis doesn't take into account the contextual use of the words (which could include instances such as "I love this fake houseplant!"). But his finding does provide a heuristic for whether or not discussions using these keywords have increased over the years.[1]

Of the reviews submitted to and analyzed by ReviewMeta from January 2015 through October 2019, mentions of the word “fake,” “counterfeit,” or “counterfiet” rose from 1.725 percent to 4.275 percent. Although the context of the usage was not analyzed, it shows a rise in the discussion about the words.

Fakespot’s Gross says the counterfeit problem is largely concentrated on a few massive sites. “I would say the majority is happening on Amazon, eBay, and Wish—those three are pretty notorious for counterfeits,” he says.

Amazon fights back

Amazon is clearly aware of the scope of the problem and is relying on technology to fight back. Given that its site scans 5 billion attempted product page changes a day, only machine learning could tackle that kind of challenge.

In addition to putting financial muscle behind legal action against counterfeiters, as well as more recently sharing information with law enforcement, Amazon says it has devoted “substantial amounts of time and resources” to proactively fighting counterfeits, including devoting “$400 million in personnel and tools built on machine learning and data science to protect our customers from fraud and abuse in our stores.”

Those programs include Brand Registry, a trademark and copyright protection system; Transparency, a system that uses QR-like codes to track individual units; Project Zero, which gives invited brands that are already part of the Brand Registry the ability to take down listings from sellers of counterfeits; Intellectual Property Accelerator, a program to help smaller brands procure early intellectual property protection; and Utility Patent Neutral Evaluation, a program that helps owners of a patent get knockoffs removed from Amazon without going through a lengthy and expensive legal process.

"I don't think it is enough yet, but I think it's great progress," says Fred Killingsworth, CEO of Hinge Global, a consulting agency that works with brands to optimize accounts on Amazon. He notes that manufacturers have not yet come up with solutions as sophisticated and comprehensive as what Amazon has implemented. However, manufacturers are also reluctant about participating in programs that not only make them more dependent on an Amazon product they have to pay for, but that give Amazon even more data about their sales.

Sumroy, the Mifold travel booster seat CEO, credits Amazon with at least trying to combat what has become an international problem. "My fear isn't Amazon, my fear is the eBays and AliExpresses and whatever crops up next," he says. Although the programs Amazon provides are more adept at stomping out copyright and trademark infringements than they are at getting rid of knockoffs, Sumroy has had success in taking down sellers who use his imagery or packaging. "We've been singularly unsuccessful with Ebay," he says. "There are no real tools with Alibaba and AliExpress, not like Amazon is trying."

How to be smarter about fakes

You can take steps to protect yourself. Take a moment before you click to buy. When you're on an e-commerce site that has a pseudonymous seller, approach the purchase with the same skepticism you would when buying something at a flea market. (Remember that this includes many items sold through Amazon Prime.) Know that what the seller has in stock may not be exactly what is pictured. Keep in mind that the seller can change when you change the zip code, color, or size on an item, so make sure you're buying from the people you want to buy from. Read any seller reviews available, as well as the reviews on the product page—but read

them all with a grain of salt. When authenticity is paramount, you may even choose to purchase directly from the manufacturer website.

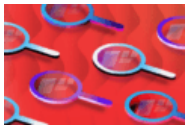
If you think you've already purchased a fake, we have advice for you, too. Read it here.

At Wirecutter, we always try to choose vendors that have high ratings and are authorized sellers, and that we've personally had good experiences with and can vouch for. Our reviews can advise you on how authentic products should look, feel, and perform. We're not infallible, but we'll always try our best to help ensure that you're actually getting a great product we recommend and not some bum knockoff. The burden of discerning authenticity should not be yours alone.

Footnotes

1. ReviewMeta's analysis included 2,509,399 products with 42,497,039 reviews in 2015, 2,544,960 products with 51,262,966 reviews in 2016, 1,241,585 products with 38,121,621 reviews in 2017, 973,724 products with 34,713,435 reviews in 2018, and 469,403 products with 23,745,568 reviews from January–October 2019. The reviews represent a percentage of what is offered on Amazon, but likely include many of the most viewed listings as the products are submitted by millions of ReviewMeta readers, according to Tommy Noonan. (ReviewMeta earns money from banner ads on its site.)

Further reading



7 Myths About Counterfeit Products, Debunked

What to Do If You Think Your Amazon Purchase Is a Fake

The Best Travel Car Seats

The Best Tweezers

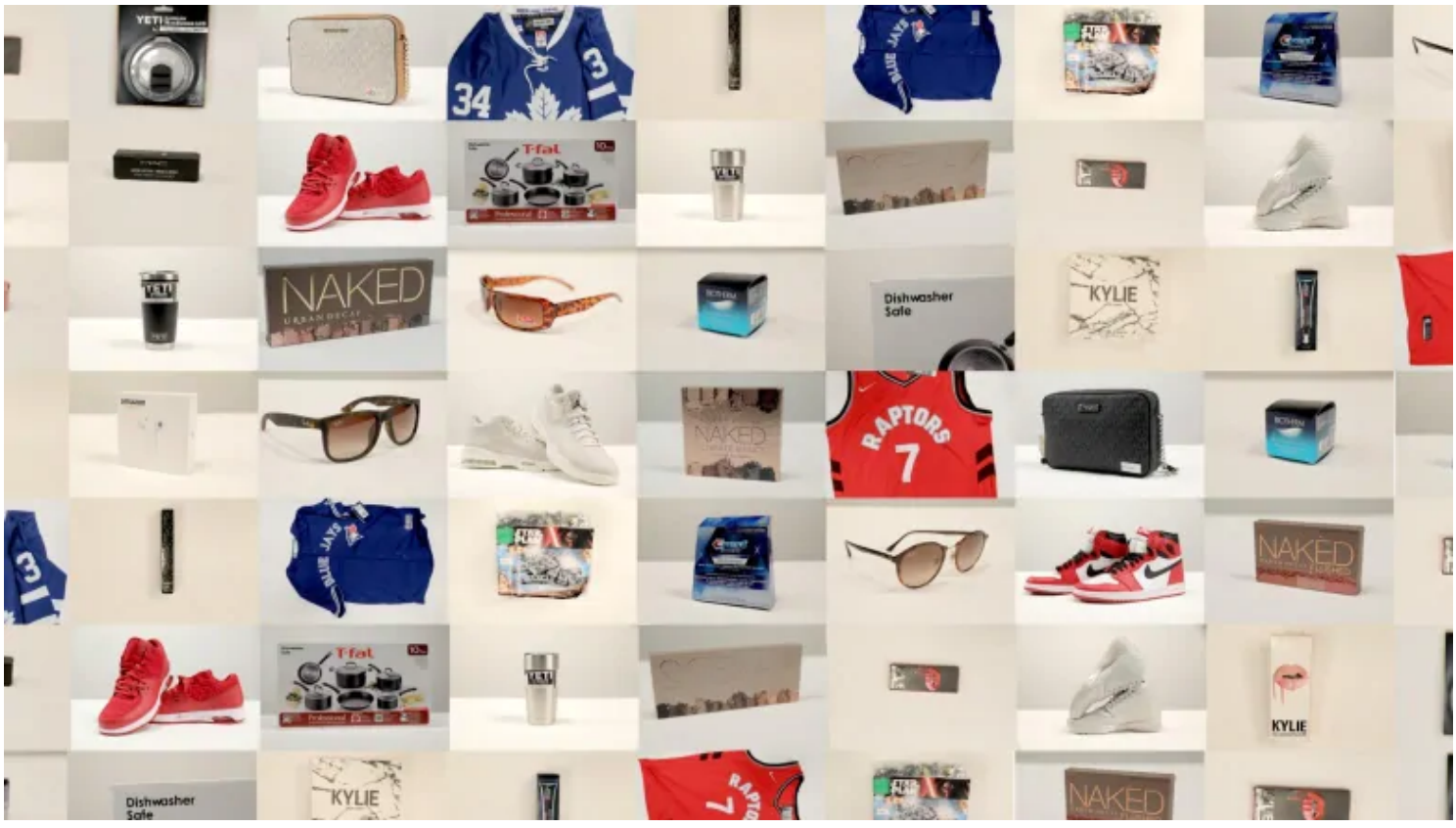
EXHIBIT 8

Business · Marketplace

We bought dozens of products from AliExpress, Amazon, eBay, Walmart and Wish. Over half were suspected fakes

Why you might want to think twice before shopping online

Jenny Cowley, Asha Tomlinson and Nelisha Vellani · CBC News ·
Posted: Feb 21, 2020 4:00 AM ET | Last Updated: February 21



Marketplace tested dozens of products purchased from popular online platforms, including AliExpress, Amazon, eBay, Walmart and Wish, finding many that were suspected to be fake by a panel of counterfeit experts. (CBC)

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

To test how prevalent counterfeits are online, *Marketplace* purchased dozens of well-known products — ranging from electronics to sportswear to cosmetics — from five popular online retailers: AliExpress, Amazon, eBay, Walmart and Wish.

Each product listing seemed legitimate, with some prices that compared to retail stores and official-looking advertisements.

More than half of the products *Marketplace* received were suspected or confirmed counterfeits, with knockoffs found on every platform.

And in some cases, *Marketplace* found that the risk of ending up with a knockoff might be more than just a financial hit.

Alarming levels of heavy metals

Some of the goods purchased by *Marketplace* were health and beauty products from multiple brands, including MAC lipstick, Crest Whitestrips, Kylie Cosmetics lip kits, Urban Decay's "Naked" eyeshadow palettes and Biotherm eye cream.

The products were then sent to a scientific lab in the Toronto area for heavy metal analysis.

Two products — both purchased from AliExpress — contained heavy metal levels exceeding Health Canada's standards for cosmetics.

The first, Mac Lustre Lipstick in Lady Danger shade was confirmed to be counterfeit by parent company Estee Lauder. One big giveaway? Lady Danger is not one of the brand's lustre shades, but rather is part of its matte line of lipsticks.

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

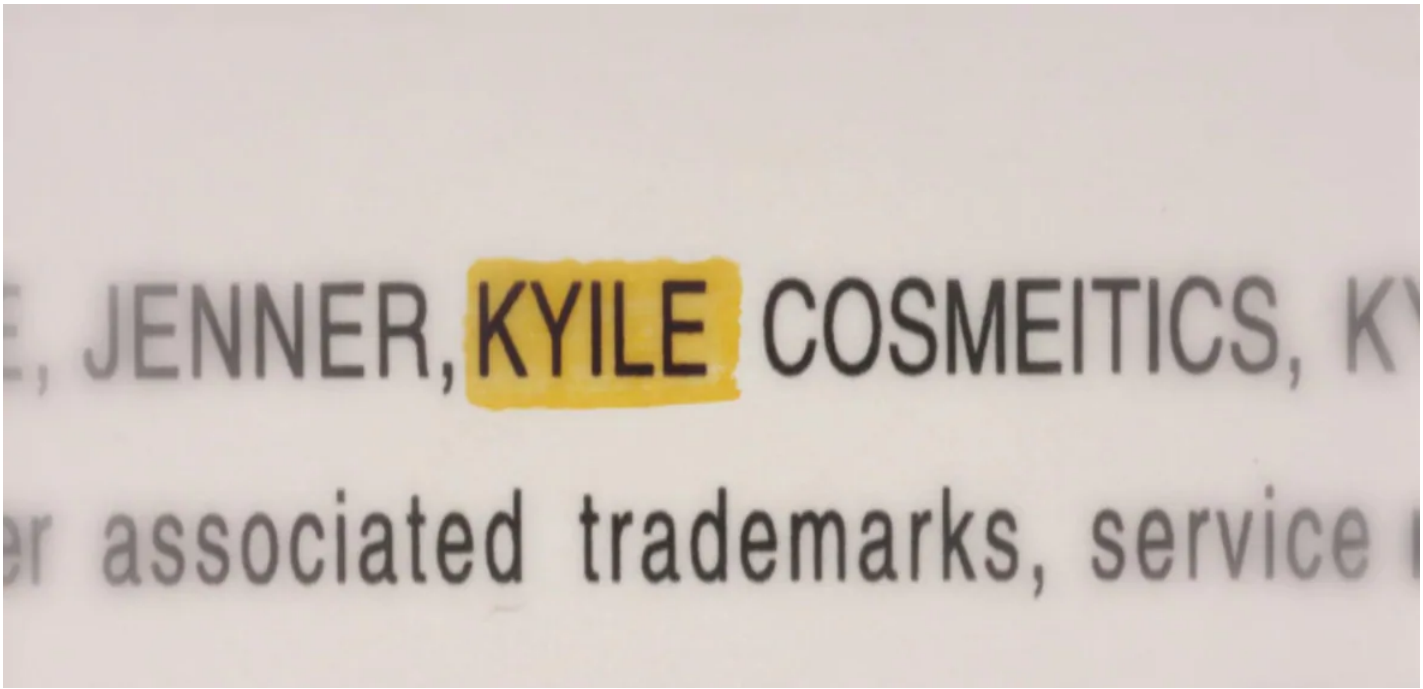
These two MAC lipsticks might look similar, but only one is real. The product on the left, purchased from AliExpress, was confirmed to be a fake. (Dave MacIntosh/CBC)

What's more, the product was found to contain 751 times the amount of lead Health Canada considers acceptable in cosmetics.

That's a big concern, says University of Guelph toxicologist Ryan Prosser, because the product goes on the lips and could be easily ingested. "It's pretty shocking," he said.

Exposure to high levels of lead could have an impact on a person's cognitive ability, he said. It's an even larger risk for children, who have still developing nervous systems.

"You could obviously expose children if they're playing with the lipstick, playing dress-up, or if they're in contact with a caregiver that's wearing lipstick," said Prosser.



Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

One of the Kylie Jenner lip kits purchased also contained a worrisome level of a heavy metal; it was found to have more than double the amount of mercury that Health Canada sees as "technically avoidable" in cosmetics.

Like lead, mercury is a neurotoxin. Increased exposure to mercury could impact the nervous system, particularly in children and pregnant women.

Jenner's company would not confirm whether the product was counterfeit, but industry experts had strong suspicions because of a glaring typo: The celebrity's name was incorrectly spelled on the back of the packaging as "Kyile." The word "cosmetics" was also spelled incorrectly.

WATCH | Marketplace's full investigation, Counterfeit Crackdown, below:

Testing Walmart, Amazon, eBay, AliExpress, and Wish. We buy 100 products - electronics, cosmetics, sports jerseys, and handbags. And we send some products to a lab to test for toxins. 22:30

Profits could be funding organized crime

The potential dangers of counterfeit goods extend well beyond makeup. Reports show that counterfeit toys, drugs, car seats, airbags and electronics have put people at risk, in some cases, even causing death.

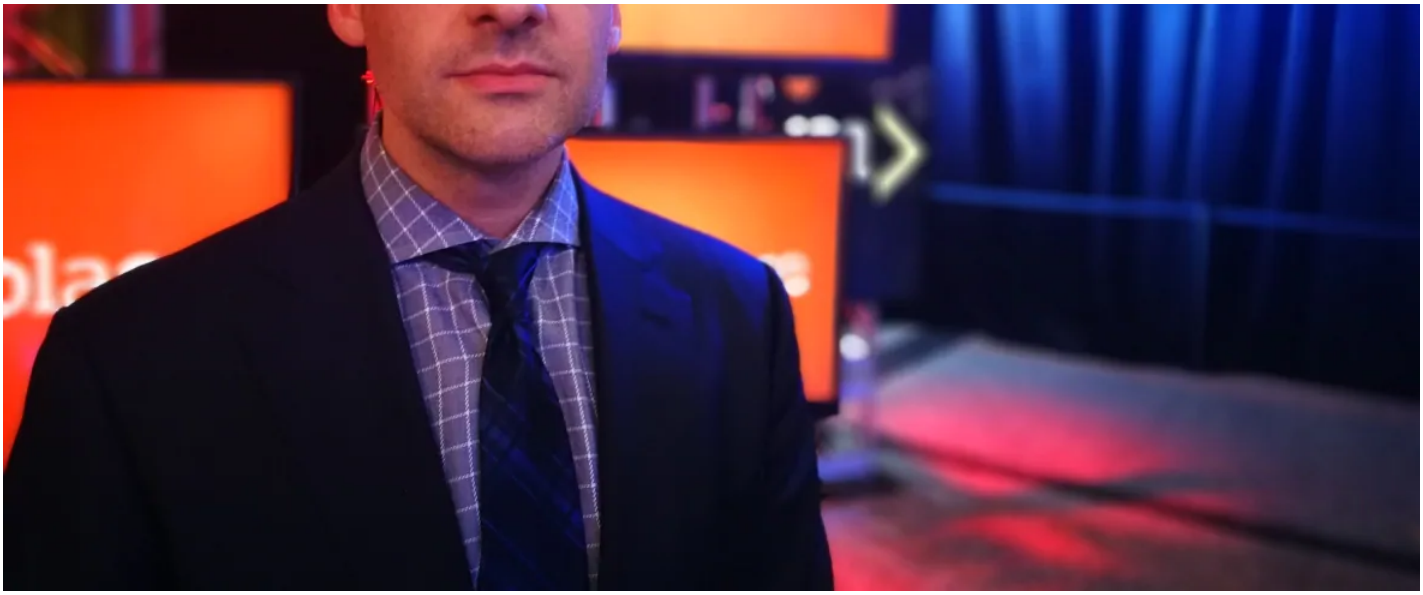
And those products that don't appear dangerous could still have severe repercussions.

Toronto-based lawyer and counterfeit expert David Lipkus notes that fakes are an industry worth hundreds of billions of dollars in North America alone.

"This impacts on organized crime and a lot of the funding goes to terrorism," he said.

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close



Think twice before you purchase knockoffs, says lawyer David Lipkus, as the proceeds from such sales are often used to support organized crime. (Jenny Cowley/CBC)

It's a concern shared by Lorrie Turner, legal counsel and senior vice-president of brand protection for headwear brand New Era Cap Co.

"All of that money is used illegitimately to support other criminal activities," she said. "While you may think it's just an individual trying to earn money, ultimately all that money goes toward nefarious things."

Interpol states on its website that there is a clear link between illicit trade of fake or pirated goods and other crime, including human trafficking, drug trafficking and money laundering.

In 2014, the United Nations Commission on Crime Prevention and Criminal Justice said that counterfeiting was the second-largest source for criminal incomes worldwide.

And in 2015, those who orchestrated the deadly attack on French satirical newspaper Charlie Hebdo raised money to buy their weapons by selling counterfeit Nike shoes on the streets of Paris.

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

In cases where there was no response from the manufacturers, three counterfeit products experts were consulted and asked to verify the products' authenticity.

A number of companies, including Apple, Fanatics, Adidas, Lego and MAC, confirmed that *Marketplace* was sold at least one counterfeit product from either AliExpress, Amazon, Ebay and Wish.

WATCH | How to identify counterfeit Raptors jerseys and fake Kylie Cosmetics lip kits:

Marketplace brought Toronto Raptors jerseys and Kylie Cosmetics to our panel of experts to learn how to spot a fake. And lab results show that some makeup we bought contains toxic ingredients. 4:25

Among the products confirmed to be counterfeit were sports jerseys, Apple Airpods, a MAC lipstick and Lego.

In the case of one pair of Apple Airpods, purchased on eBay, the product was determined to be legitimate but Apple confirmed it had counterfeit packaging and a third-party lightning cable. They were described in the online listing as "manufacturer refurbished," which Apple said was untrue.

Five of the products purchased — three packages of Crest WhiteStrips and two cellphone chargers — could not be verified, mainly due to missing packaging. Crest advises that consumers should only purchase Crest Whitestrips when they are in a sealed box.

99,500 vs. 69 shipments stopped

After *Marketplace* was easily able to order a number of suspected and confirmed counterfeit products online, we set out to discover what Canada's border agency was doing to stop such shipments.

But a request made under the Access to Information Act revealed that between June 2015 and

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

These products were seized by U.S. Customs and Border Protection in Buffalo, N.Y. (CBC)

The low number of detained shipments is perhaps surprising, given that Canada introduced a law — the Combating Counterfeit Products Act — in 2014 that "enables customs officers to detain goods that they suspect infringe copyright or trademark rights."

"Our approach is different from that of the U.S. in that our interdiction focus is on health safety and security threats," the CBSA said in a statement.

Annual stoppages at the border appear to be increasing: CBSA told *Marketplace* they detained 63 shipments between April and September 2019.

Lipkus is glad there's more action, but says it's also clear there's still work to be done.

- **Canada seizing few shipments of fake goods despite law targeting counterfeits**

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

"There's no question that the United States is doing more. And there's no question that Canada and our amazing border officers need more money and resources to address this issue so the numbers increase."

That's not the only criticism Canada has received from others fighting counterfeits.

The Office of the United States Trade Representative releases a list of "notorious markets" annually, which lists major markets around the world where copyright infringement and counterfeit trade takes place.

These shoes, found at Pacific Mall in Markham, Ont., are meant to be Valentinos. But take a closer look at the spelling. (Jenny Cowley/CBC)

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

recklessly making false representation to the public and selling or distributing goods in association with a trademark. One of those people was also charged with possession of proceeds of crime.

Marketplace visited the mall almost one year after the initial raid and found many goods were openly being sold as knockoffs. A followup visit earlier this month confirmed fakes were still on many store shelves.

When producers visited Pacific Mall in Markham, Ont., they found dozens of counterfeit designer products being openly sold. (Nathan Denette/Canadian Press)

In addition to consumers seeking out authorized retailers, store owners also need to have more of a role in verifying their products, Lipkus said.

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

A spokesperson for Pacific Mall said consumer health and safety is a top priority for the shopping outlet, and they believe the sale of counterfeits at the mall is extremely limited.

They also said they issue warnings to store owners, and work with manufacturers and local police to help identify fakes.

Canada's counterfeit problem

When *Marketplace* enlisted industry experts to help point out potentially counterfeit products, they pointed out reasons such as stitching, typos, quality, and serial numbers.

Experts suspected fakes on every platform *Marketplace* purchased from.

Walmart disputed the findings, but all companies said that they are committed to stopping and preventing the sale of counterfeit goods on their platforms.

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

Experts say when trying to spot a fake, look at small details. On this Toronto Maple Leafs jersey, confirmed counterfeit by Reebok, stitching connects all the letters. The suspected counterfeit Michael Kors purse has an uneven emblem and a misprint on the fabric. The Blue Jays jersey, confirmed counterfeit by Majestic, has odd stitching when turned inside-out. (CBC)

Experts are reluctant to share some tips, as not to tip the counterfeiters off, but there are some things consumers can do if they suspect they may have purchased a counterfeit.

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

"We were expecting our third and we thought, 'Well, let's get a couple more sound machines, one for each of the kids' rooms,'" he said.

- **Nike calls off pilot program with Amazon ending direct sales**

Folks purchased the same model he had previously bought, from a seller listed as "MARPAC," the brand name of the sound machine.

But when he plugged the new machine in to test it, he quickly noticed a difference in quality: it was weaker than his other devices.

Folks reached out to Marpac directly, which confirmed the machines were counterfeit.

"What bothered me the most was the fact that this ran through Amazon Prime," said Folks. "It also had an 'Amazon's Choice' stamp on the page, which to me seems like it'd been vetted."

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

Amazon apologized, promising it wouldn't happen again, and sent Folks a link that they said was real.

He ordered again, and a few days later the machines arrived. This time, something was familiar about the packaging.

"I opened the box [and] I noticed right away that there was a little rip in one of the boxes," he said. "And when I put the last ones away that I shipped back with my first order, I had ripped the box in a particular spot."

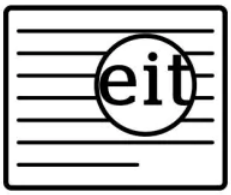
Checking the serial numbers, Folks and Marpac were able to confirm that these machines were also counterfeit — and Folks suspected they were the exact ones he just sent back.

Amazon's executive customer service team said it was investigating, but Folks says he hasn't heard anything since.

"I'm shocked. They're sending out counterfeit goods and they seem to want to do nothing with them," he said. "How many other people is this happening to?"

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close



Look for typos, especially in the product's ingredients and in the French text, if it has it.

Look at the quality of stitching and how details, like purse straps, are attached.

Check for hologram tags on some products, like official sportswear or Canada Goose jackets.

Reach out to the official brand for clarification.

If you think you've received a counterfeit, contact the Canadian Anti-Fraud Centre.

Part of the reason why Folks could have received a counterfeit machine is because third-party

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

To avoid falling victim to counterfeits, Lipkus recommends consumers purchase their products directly from authorized sellers and not through third-party marketplaces.

Lipkus also points to the Canadian Anti-Fraud Centre's Project Chargeback, which partners with credit card companies to fight counterfeiting. If you report your purchase and the address you bought it from, you could get a refund.

"But more importantly," said Lipkus, "it could trigger an investigation into the merchant."

POPULAR NOW IN NEWS

1 **Canadians have made 190,000 repayments on CERB claims, says CRA**
1067 reading now

2 **Wendy Mesley suspended from hosting after using 'careless' language in discussing racial issue**
622 reading now

3 UPDATED
Alberta focused on return to 'near-normal' classes to start 2020-21 school year
394 reading now

4 **For 5th day in a row, no COVID-19-related deaths in B.C.**
366 reading now

5 **Canada-U.S. border closure to be extended beyond June 21, sources say**
359 reading now

RECOMMENDED FOR YOU

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

says CRA

Kathleen Harris

News - Politics

language in discussing racial issue

News - Canada

sources say

Katie Simpson

News - Canada

Starbucks to close as many as 200 stores in Canada even after COVID-19

Pete Evans

News - Business

VIDEO

Widowed by COVID-19, a pregnant mother of 5 struggles with guilt and grief

Daniel Boily

News - Canada - Montreal

©2020 CBC/Radio-Canada. All rights reserved.

Visitez Radio-Canada.ca

Please know that cookies are required to operate and enhance our services as well as for advertising purposes. We value your privacy. If you are not comfortable with us using this information, please review your settings before continuing your visit.

Learn more Close

EXHIBIT 9

Intellectual Property Rights

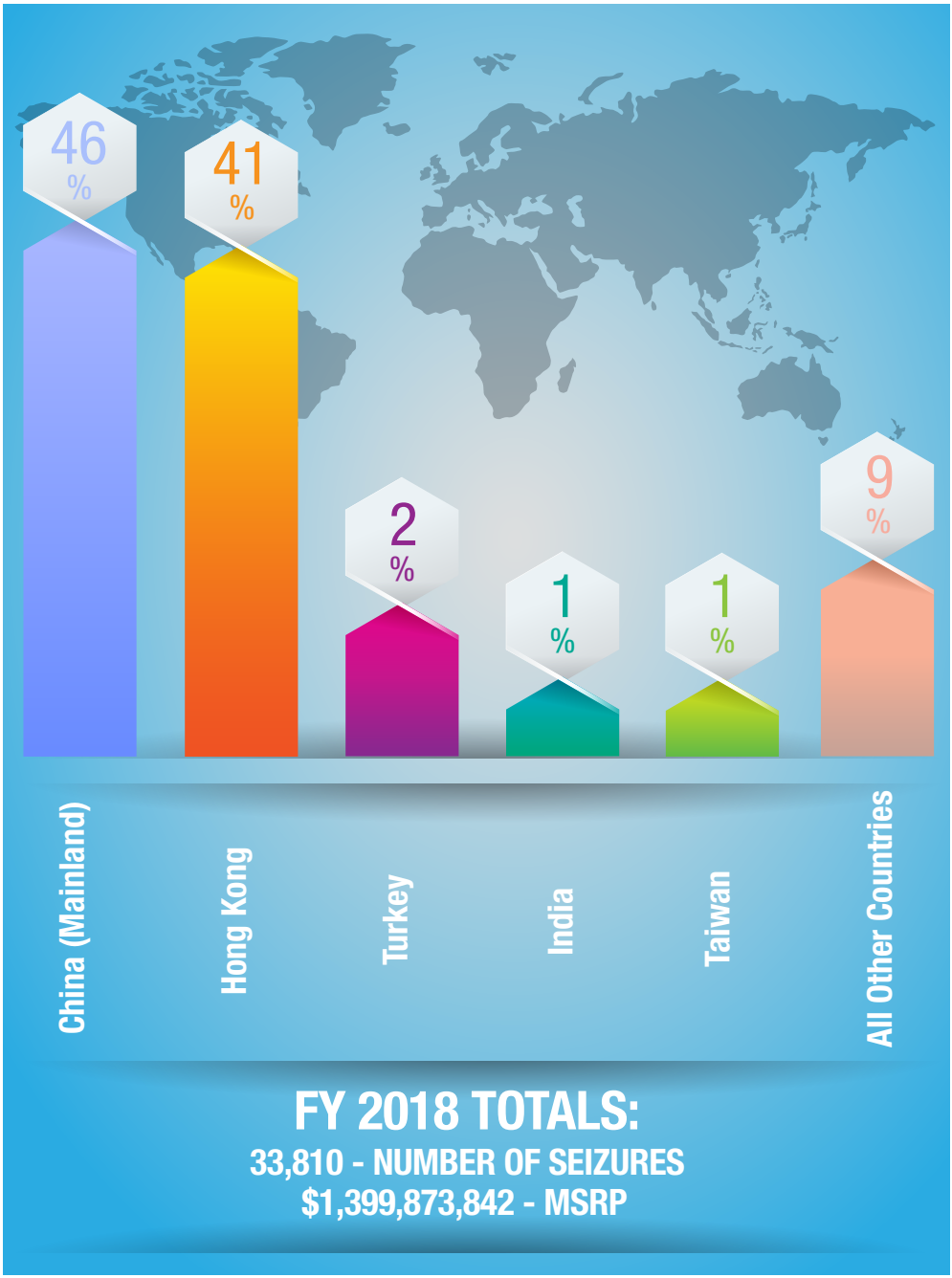
Fiscal Year 2018 Seizure Statistics

Prepared by

U.S. Customs and Border Protection
Office of Trade

Homeland Security

FISCAL YEAR 2018 IPR SEIZURE STATISTICS
BY NUMBER OF SEIZURES



FY 2018 TOTALS:

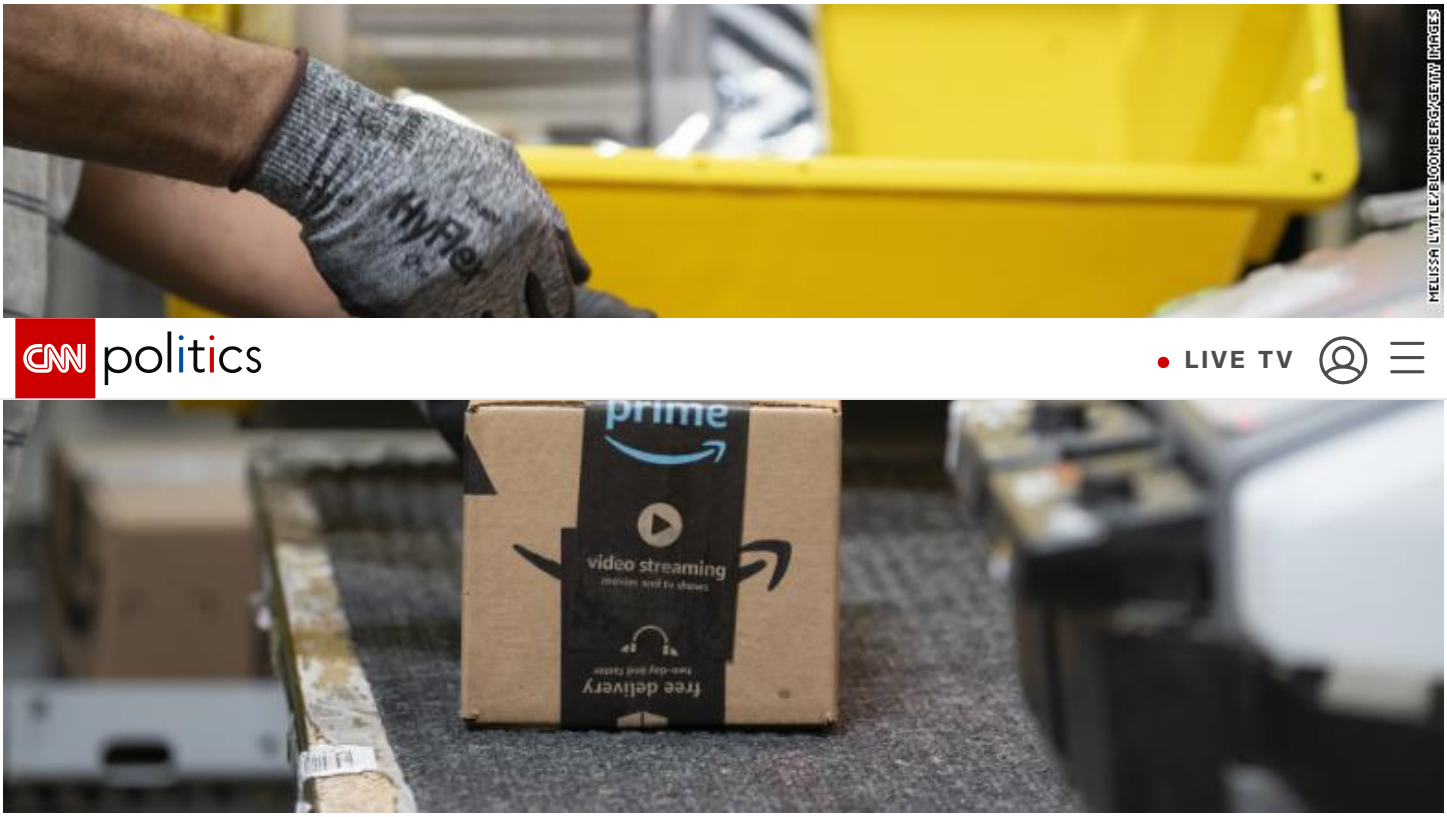
33,810 - NUMBER OF SEIZURES

$1,399,873,842 - MSRP

EXHIBIT 10

Administration wants online retailers to do more to police counterfeit goods

By Geneva Sands, CNN
Updated 8:23 PM ET, Fri January 24, 2020



In this April 30, 2019, file photo, an employee places a label on a box at the Amazon.com Inc. fulfillment center in Baltimore.

(CNN) — Officials from the Department of Homeland Security and the White House said Friday that they are taking steps to shift more of the burden of tackling counterfeit goods to e-commerce hubs like Amazon, a response to an April 2019 presidential memo.

Peter Navarro, director of the White House Office of Trade and Manufacturing Policy, said the shift is needed because the onus and cost have been on the government and intellectual property rights holders to "police the internet" for counterfeit goods.

"It just can't work that way," he said during a news conference Friday to announce the plans.

The United States loses $300 billion to $500 billion a year to intellectual property theft, Navarro said Friday.

He said that "for all practical purposes, these e-commerce hubs are basically laundries for counterfeiting" and the "thrust here of these recommendations is to get these e-commerce hubs to accept their share of the responsibility."

He said the strategy is to "shift the burden to the places where the burden needs to be adopted," such as hubs like Amazon, eBay and Alibaba.

Navarro also said the administration also plans to target people offshore who "can't be touched now."

Amazon issued a statement Friday acknowledging that trust is difficult to earn but pushing back on the idea that it has not accepted responsibility. A spokesperson said Amazon has invested more than $400 million to "protect our store from fraud, including counterfeit or non-compliant products."

"We already have programs and processes that go well beyond our obligations under US law," the statement said. "Our efforts have ensured that over 99% of the products our customers view on Amazon never receive a complaint about counterfeits. Beyond blocking fraudsters from our store, we also work closely with brands and law enforcement to hold bad actors accountable offline, including both civil and criminal law suits."

Last April, President Donald Trump had instructed DHS to compose a report in conjunction with the Commerce Department, the attorney general and other federal agencies with recommendations for combating counterfeit goods in the American marketplace within 210 days.

Asked at the time whether Trump's memo had anything to do with the President's animus for Amazon CEO Jeff Bezos, Navarro replied, "Zero."

"Despite public and private efforts to-date, the online availability of counterfeit and pirated goods continues to increase," reads the report, released Friday.

Acting Homeland Security Secretary Chad Wolf said Friday that the solution to the problem of pirated and

"Today's report, where appropriate, shifts the burden to the private sector," said Wolf. "International e-commerce sellers must step up and do more."

Wolf said the private sector must "aggressively self-police and focus their innovation and expertise" on the issue, adding that the department would continue its work with the industry and seek feedback.

Wolf also called on consumers to inform themselves about the risks associated with counterfeit goods.

CNN's Clare Sebastian contributed to this story.

Search CNN...

US

World

Politics

Business

Opinion

Health

Entertainment

Tech

Style

Travel

Sports

Videos

Coupons

More

Weather

CNN politics

CNN politics

• LIVE TV

FOLLOW CNN POLITICS

Terms of Use Privacy Policy Do Not Sell My Personal Information AdChoices About Us CNN Studio Tours
CNN Store Newsletters Transcripts License Footage CNN Newsource Sitemap

© 2020 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.
CNN Sans ™ & © 2016 Cable News Network.

EXHIBIT 11

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.

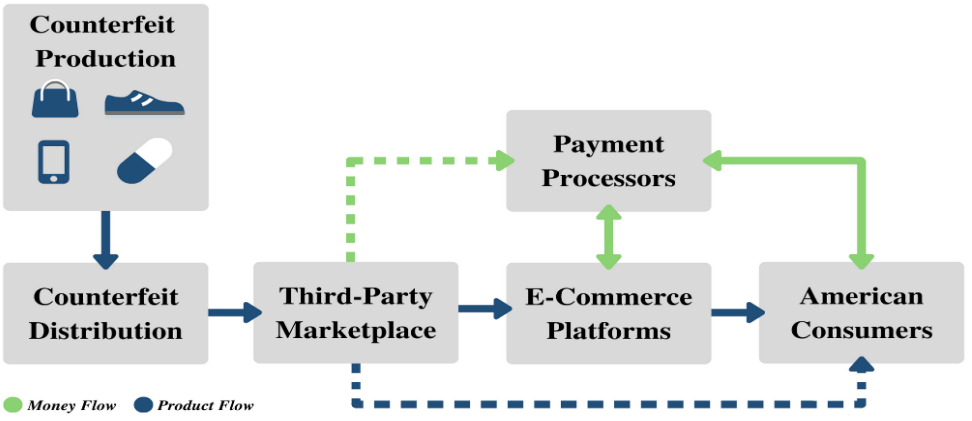
For counterfeiters, production costs are low, millions of potential customers are available online, transactions are convenient, and listing goods on well-known platforms provides an air of legitimacy. When sellers of illicit goods are in another country, they are also exposed to relatively little risk 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/

EXHIBIT 12

SECTION II: Country Reports

PRIORITY WATCH LIST

EAST ASIA AND THE PACIFIC

CHINA

China remains on the Priority Watch List in 2019, and is subject to continuing Section 306 monitoring.

Ongoing Challenges and Concerns

Despite a broad government reorganization, including of intellectual property (IP) responsibilities among government agencies, and proposed revisions to IP laws and regulations, China failed to make fundamental structural changes to strengthen IP protection and enforcement, open China's market to foreign investment, allow the market a decisive role in allocating resources, and refrain from government interference in private sector technology transfer decisions. For U.S. persons who rely on IP protection in what is already a very difficult business environment, severe challenges persist because of gaps in the scope of IP protection, stalled legal reforms, and weak enforcement channels.

As part of an investigation under Section 301 of the Trade Act of 1974 on policies and practices related to technology transfer and IP, the United States found that China has engaged in a range of unfair and harmful conduct, including investment and other regulatory requirements that require or pressure technology transfer, discriminatory licensing restrictions, direction or facilitation of the acquisition of foreign companies and assets by domestic firms to obtain cutting-edge technologies, and conducting and supporting unauthorized intrusions and theft from computer networks of U.S. companies to obtain unauthorized access to IP. The Section 301 investigation and remedies have prompted numerous high-level discussions between the United States and China, which are ongoing.

High-profile statements in support of IP and innovation by Chinese government officials are no substitute for real structural changes to address shortcomings in China's IP system, which cannot be excused by the country's stage of economic development. The United States, other countries, and the private sector continue to urge China to embrace meaningful and deep reform to its IP-related legal and regulatory framework. The results to date have represented missed opportunities to address priority concerns of the United States and others, including where China's proposed revisions to legal and regulatory measures fail to adopt U.S. recommendations for reform. Necessary progress will not be achieved unless China can demonstrate its resolve to protect and enforce IP rights. For these reasons, as elaborated below, China remains a precarious and uncertain environment for U.S. right holders.

Developments, Including Progress and Actions Taken

As discussed below, although China has reorganized its IP protection and enforcement authorities and proposed draft amendments to certain IP-related legal and regulatory measures, these steps toward reform fall short of needed fundamental changes to the IP landscape in China.

In March 2018, China instituted broad changes to the organization of ministries and agencies responsible for the protection and enforcement of IP. China created a new State Administration for Market Regulation (SAMR), which centralized responsibilities for administrative enforcement of patents and trademarks, enforcement of the Anti-Monopoly Law, regulatory approval of pharmaceutical products, and standardssetting, among other responsibilities. The China Trademark Office was moved under the State Intellectual Property Office (SIPO) and took on the administration of China's geographical indication (GI) system. SIPO moved under the newly created SAMR, and is now known as the China National Intellectual Property Administration (CNIPA). As a separate part of the reorganization, the National Copyright Administration moved from the State Administration of Press, Publication, Radio, Film, and Television to the Central Propaganda Department of the Communist Party of China. The drug and medical device related components of China's Food and Drug Administration became the National Medical Products Administration. Given their recent completion, it is too soon to determine whether these efforts to reorganize and centralize administration and enforcement of IP will be positive for right holders.

China has continued with judicial reforms in the past year. The most prominent change was the establishment of a new appellate tribunal within the Supreme People's Court (SPC), titled the "SPC IP Court," on January 1, 2019. The new SPC IP Court has jurisdiction over appeals of decisions from lower courts in technically-complex IP cases, as well as appeals of certain administrative enforcement decisions. As the three intermediate-level specialized IP Courts reportedly demonstrate competence, expertise, and transparency to a greater degree than other Chinese courts, the SPC IP Court is a promising step for improved consistency in outcomes. After the establishment of the Hangzhou Internet Court, which typically addressed disputes arising from Internet services in half the time as conventional courts, China created two new Internet courts in Beijing and Shanghai. Notwithstanding these positive developments, U.S. right holders report that procedural obstacles to appealing decisions of the CNIPA Trademark Adjudication Board to the Beijing IP Court are sometimes insurmountable and may discourage appeals altogether. A broader concern is intervention by local government officials, party officials, and powerful local interests, which undermines the independence of the courts and rule of law. A truly independent judiciary is critical to promote rule of law in China.

In addition to insufficient judicial independence in certain cases, right holders continue to report that burdensome thresholds for criminal enforcement, onerous authentication and other evidentiary requirements, lack of means to require evidence production, insufficient damage awards, and lack of deterrent-level statutory damages and criminal penalties all undermine the effectiveness of China's court system for addressing IP infringement.

Trade Secrets

China's 2017 amendment of the Anti-Unfair Competition Law (AUCL) went into effect on

January 1, 2018. The amended AUCL represented a major missed opportunity to address critical concerns, including the overly narrow scope of covered actions and actors, the failure to address obstacles to injunctive relief, and the need to allow for evidentiary burden shifting in appropriate circumstances.

One particular area for continued monitoring is the availability of preliminary injunctions in trade secret and other IP disputes. A new judicial interpretation, titled the "Provisions of the Supreme People's Court Regarding Certain Issues Concerning the Application of Law During the Examination of Act Preservation in Intellectual Property and Competition Disputes," went into effect on January 1, 2019. It remains unclear whether, in practice, this judicial interpretation will enable right holders to obtain timely preliminary injunctions against all categories of trade secret misappropriation.

China should not only address these shortcomings, but also issue guiding court decisions to improve consistency in judicial decisions on trade secrets. Reforms also should prevent the disclosure of trade secrets and other confidential information submitted to government regulators, courts, and other authorities, and address obstacles to criminal enforcement.

Manufacturing, Domestic Sale, and Export of Counterfeit Goods

China continued to be the world's leading source of counterfeit goods, reflecting its failure to take decisive action to curb the widespread manufacture, domestic sale, and export of counterfeit goods. According to a 2019 Organisation for Economic Co-operation and Development (OECD) report, China together with Hong Kong, through which Chinese merchandise often transships, continued to account for over 80 percent of seizures of counterfeit and pirated goods worldwide.[16] Applying a different methodology, another analysis from the 2019 OECD report analyzed 2016 data and estimated that China and Hong Kong were the source of $322 billion in fake exports, around 63.4 percent of the global total.[17] This massive problem impacts not only the interests of IP right holders, but also poses health and safety risks. Right holders report that the production, distribution, and sale of counterfeit medicines, fertilizers, pesticides, and under-regulated pharmaceutical ingredients remain widespread in China.

China has not shown significant progress in addressing the registration of trademarks in bad faith, despite a number of announcements by China's State Administration for Industry and Commerce (SAIC) in September 2017. For many years, U.S. brand owners have reported that third parties are registering large numbers of trademarks that are identical to, substantially indistinguishable from, or similar to, existing U.S. brands. As a result, third parties are able to obtain trademarks in China in bad faith even when the U.S. trademark is famous or well-known, and the resulting registrations damage the goodwill or interests of U.S. right holders. The use of these trademarks is also likely to confuse Chinese consumers who may be unaware that a Chinese trademark is used for goods and services that are not connected with the U.S. right holder. In February 2019, CNIPA issued for comment a new draft measure, titled "Provisions on Regulating the Registration of Trademark Applications," to combat "abnormal" applications, including applications submitted in

[16] *Trends in Trade in Counterfeit and Pirated Goods,* at 27-28, available at https://euipo.europa.eu/ohimportal/en/web/observatory/trends-in-trade-in-counterfeit-and-pirated-goods.
[17] *Id.* at 46.

bad faith. The United States has provided China detailed comments on the draft, identifying the need to clarify key provisions and include additional actions if it is to help curb bad faith trademark registrations in China. Other critical reforms should be addressed by amendments to the Trademark Law and related implementing regulations.

E-Commerce Piracy, Counterfeiting, and Other Issues

As China has become the largest e-commerce market in the world, widespread online piracy and counterfeiting in e-commerce markets represent critical concerns for U.S. right holders. According to published reports, online retail sales in China are expected to grow to $1.9 trillion in 2019.[18] OECD reports have noted that the growth of small parcels carrying counterfeit and pirated goods reflected the move from offline to online sales,[19] and China together with Hong Kong have been the leading source of seized counterfeit goods shipped by mail or express couriers.[20] Right holders report that online sellers of counterfeit goods often advertise that orders will be fulfilled via China Post's express mail service and exploit the high volume of packages to the United States to escape enforcement. Furthermore, although some leading online sales platforms have reportedly streamlined procedures to remove offerings of infringing articles and enhanced cooperation with stakeholders to improve criminal and civil enforcement of IP, right holders continue to express concerns about ineffective takedown procedures, slowness to respond to small and medium-sized enterprises (SMEs), and insufficient measures to deter repeat infringers. Other right holders report growing online piracy in the form of thousands of "mini Video on Demand" (VOD) locations that show unauthorized audiovisual content and online platforms that disseminate unauthorized copies of scientific, technical, and medical journal articles and academic texts. A range of such concerns led to the re-listing of DHgate.com and Alibaba online sales platform Taobao as notorious markets in the 2018 Out-of-Cycle Review of Notorious Markets (*Notorious Markets List*), as well as the first-time listing of Pinduoduo.com.

The new E-Commerce Law took effect on January 1, 2019. Despite extensive U.S. engagement regarding drafts of the law, China failed to address major concerns regarding provisions that would impose burdensome requirements on right holders seeking to enforce their IP, while allowing infringing sellers to halt takedown procedures through submission of counter-notifications that lack sufficient information to ensure their validity and without penalties for submissions in bad faith. It is critical that the E-Commerce Law, as implemented, does not undermine the existing framework for Internet service provider notices of copyright infringement and cease-and-desist letters. A further negative signal was the issuance of a draft Tort Liability Chapter of the Civil Code that contained similar provisions to problematic portions of the E-Commerce Law. The final version of the Tort Liability Chapter should implement a predictable legal environment that promotes effective cooperation among interested parties in deterring online copyright infringement.

[18] *Chinese Retail Sales Are Set to Dwarf U.S. Sales This Year* (Jan. 23, 2019), available at https://www.washingtonpost.com/business/2019/01/23/chinese-retail-sales-are-set-dwarf-us-sales-this-year/.
[19] *Trends in Trade in Counterfeit and Pirated Goods*, at 19-20, available at https://euipo.europa.eu/ohimportal/en/web/observatory/trends-in-trade-in-counterfeit-and-pirated-goods.
[20] *Misuse of Small Parcels for Trade in Counterfeit Goods*, at 42-43, available at https://euipo.europa.eu/ohimportal/en/web/observatory/trade-in-fakes-in-small-parcels.

In 2018, China again failed to reform measures that bar or limit the ability of foreign entities to engage in online publishing, broadcasting, and distribution of creative content, such as prohibitions in the Foreign Investment Catalogue and requirements that state-owned enterprise hold an ownership stake in online platforms for film and television content. Right holders report that growing advance approval requirements and other barriers have reduced the availability of foreign television content and prevented the simultaneous release of foreign content in China and other markets. Collectively, these measures create conditions that result in greater piracy and a market that is less open than others in terms of foreign content and foreign entity participation. Additionally, it is critical that China fully implement the terms of the 2012 U.S.-China Memorandum of Understanding regarding films and abide by its commitment to negotiate additional meaningful compensation for the United States.

As a leading source and exporter of systems that facilitate copyright piracy, China should take sustained action against websites containing or facilitating access to unlicensed content, illicit streaming devices, and piracy apps that facilitate access to such websites. Short-lived campaigns are no substitute for deterrent-level criminal sanctions to combat online piracy and the circumvention of technological protection measures used to protect licensed content.

Need to Promote Innovation through Sound Patent and Related Policies

On January 4, 2019, China released a new draft of amendments to the Patent Law. Promising provisions include extension of the design patent term, availability of increased punitive damages for willful patent infringement, and discretionary authority for a court to order production of damages-related evidence. However, strong concerns remain about the presence of competition law concepts in the draft law, an undue emphasis on administrative enforcement, and the absence of critical reforms, as described below.

Major challenges confront pharmaceutical innovators attempting to protect and enforce their IP rights in China. Despite revisions to China's patent examination guidelines in April 2017, pharmaceutical innovators report that they are not permitted to rely on supplemental data on a consistent basis to satisfy relevant requirements for patentability during patent examination proceedings, patent review proceedings, and judicial proceedings. This practice leads to application denials, or the invalidation of existing patents, even when counterpart patents are granted by other major patenting offices. China also continues to impose unfair and discriminatory conditions on the effective protection against unfair commercial use, as well as unauthorized disclosure, of test or other data generated to obtain marketing approval for pharmaceutical products. China provides such protection only if the drug in question has not previously received marketing authorization outside China, which is an unfair and discriminatory condition that is unrelated to the purpose of such protection. Despite issuing for comment draft opinions and amendments to measures, China also has failed to establish an effective mechanism for the early resolution of potential pharmaceutical patent disputes. China additionally has failed to provide patent term extensions to compensate for unreasonable delays that occur in granting a patent (a concern not limited to pharmaceutical patents) or in relation to marketing approvals. Draft amendments to the Patent Law to provide for such extensions in relation to marketing approvals were unsatisfactory in part because extensions would be available only to patent holders that file for marketing approval of a pharmaceutical simultaneously in China and another jurisdiction. The

draft amendments failed to provide extensions for patent office delays and granted extensions only on a discretionary basis without a clear elaboration of the factors governing such a determination. China should also address delays, a lack of transparency, and inadequate engagement with pharmaceutical suppliers in government pricing and reimbursement processes.

China must address each of these concerns to better promote pharmaceutical innovation and bring China into closer alignment with the practices of other major patenting jurisdictions. In addition, China should address continuing problems with the difficulty in obtaining evidence of infringement, the disclosure obligations in standards-setting processes, the failure to clarify that a patentee's right to exclude extends to manufacturing for export, and the need to harmonize China's patent grace period and statute of limitations with international practices.

On November 21, 2018, three dozen Chinese ministries and authorities issued a memorandum of understanding imposing "social credit system" penalties for certain categories of patent-related conduct, including repeated infringement of an adjudicated patent and misconduct in the course of patent prosecution. The United States objects to any attempt to expand the "social credit system" in the field of intellectual property.

The Standardization Law took effect on January 1, 2018, and China subsequently issued draft administrative measures for the management of mandatory standards and final administrative measures for management of association standards. These measures nonetheless failed to establish that standards-setting processes are open to domestic and foreign participants on a non-discriminatory basis and provide sufficient protections for standards-related copyright and patent rights.

In 2018, Chinese authorities indicated that draft guidelines for Anti-Monopoly Law (AML) enforcement, as it relates to IP rights, have been approved for issuance. In January 2019, China published for public comment draft Rules for the Prohibition of Abuse of Market Dominance Conduct, specifying that the ownership of IP and refusal to enter transactions are factors to examine. These draft provisions heighten concerns that China's competition authorities may continue to target foreign patent holders for AML enforcement and use the threat of enforcement to pressure U.S. patent holders to license to Chinese parties at lower rates, despite the United States repeatedly expressing strong concerns regarding this practice. It is critical that China's AML enforcement be fair, transparent, and non-discriminatory; afford due process to parties; focus only on the legitimate goals of competition law; and not be used to achieve industrial policy goals.

Pending Copyright Law Amendments

Chinese authorities have indicated that they made progress toward draft amendments of the Copyright Law, but no draft has been published. It is critical to address major deficiencies in China's copyright framework, such as the failure to provide deterrent-level remedies and penalties, protection against unauthorized transmission of sports and other live broadcasts, and effective criminal enforcement, including amendments to the Regulations on the Transfer of Alleged Criminal Cases by Administrative Enforcement Organs to adopt a "reasonable suspicion" threshold for the transfer of administrative cases to criminal investigation and prosecution.

China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation

On March 22, 2018, based on an investigation in response to a Presidential memorandum, the United States Trade Representative issued a detailed report that supports a finding that China's acts, policies, and practices that force or pressure U.S. right holders to transfer technology and IP are unreasonable or discriminatory and burden or restrict U.S. commerce, and are thus actionable under section 301(b) of the 1974 Trade Act. In particular:

1. China uses foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, and various administrative review and licensing processes to require or pressure technology transfer from U.S. companies.

2. China's regime of technology regulations forces U.S. companies seeking to license technologies to Chinese entities to do so on non-market-based terms that favor Chinese recipients.

3. China directs and unfairly facilitates the systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies to obtain cutting-edge technologies and IP and generate the transfer of technology to Chinese companies.

4. China conducts and supports unauthorized intrusions into, and theft from, the computer networks of U.S. companies to access their sensitive commercial information and trade secrets.

The President directed the United States Trade Representative to take all appropriate actions under Section 301 to address the referenced acts, policies, and practices of China that are unreasonable or discriminatory and that burden or restrict U.S. commerce.

Pursuant to sections 301(b) and (c) and direction from the President, and after the submission of written comments by interested parties and public hearings, the United States Trade Representative imposed increased tariffs on certain goods of Chinese origin in several tranches. The President also directed the Secretary of the Treasury to address concerns about investment in the United States directed or facilitated by China in industries or technologies deemed important to the United States. In November 2018, the United States Trade Representative issued another detailed report, explaining that China had not fundamentally altered the unfair, unreasonable, and market-distorting policies and practices that were the subject of the March 2018 report. In December 2018, at a meeting between the President and China's President Xi Jinping in Buenos Aires, the United States agreed to hold off on raising the duty rate on certain goods while the two sides engaged in intensive negotiations for 90 days on the structural changes needed in China's trade regime. On February 24, 2019, in light of progress in discussions with China, the President directed the United States Trade Representative to postpone the increase in tariffs scheduled for March 2, 2019.

In March 2018, the USTR also initiated dispute settlement proceedings at the World Trade Organization (WTO) to address China's discriminatory licensing practices, a concern highlighted

repeatedly in past Special 301 Reports. Consultations took place in July 2018, a panel was established to hear the case in November 2018, and the United States filed its first written submission in March 2019.

China's "Secure and Controllable" Policies

Since enacting its Cybersecurity Law (CSL) in 2017, China has taken multiple steps backward through its efforts to invoke cybersecurity as a pretext to force U.S. IP-intensive industries to disclose sensitive IP to the government, transfer it to a Chinese entity, or both. Through draft and final measures, China has often applied the poorly-defined concept of "secure and controllable" information communications technology (ICT) products and services and associated "risk" factors as a putative justification for erecting barriers to sale and use in China.

On June 27, 2018, China released draft Cybersecurity Classified Protection Regulations (CCPR), which represent a continuation of the Multi-Level Protection Scheme requirements that, among other restrictions, limit procurement of software and other ICT products for purportedly sensitive systems to those containing indigenous Chinese IP. The CCPR imposed restrictions on networks operating within China, such as requiring that certain systems be connected with the Public Security Bureau system and that technical maintenance be performed within China. In September 2018, the Ministry of Public Security released the Internet Security Supervision and Inspection Provisions by Public Security Organs, which authorized public security authorities to enforce the CSL. As previously reported, pursuant to the CSL, China may require disclosure of critical source code and IP to government authorities, require IP rights be owned in China, require associated research and development be conducted in China, and curtail or prohibit cross border data flows in sectors such as cloud services.

Right holders continue to report strong concerns about other draft and final measures, particularly requirements for public disclosure of enterprise standards under the amended Standardization Law. The draft standards published by the National Information Security Standardization Technical Committee (TC-260) would assign scores to ICT products based on inappropriate benchmarks (*e.g.*, the extent to which a party discloses sensitive IP). The draft Encryption Law would impose severe restrictions on foreign businesses to keep them from competing in the commercial cryptography market.

U.S. right holders should not be forced to choose between protecting their IP against unwarranted disclosure and competing for sales in China. Going forward, China must not invoke security concerns in order to erect market access barriers, require the disclosure of critical IP, or discriminate against foreign-owned or -developed IP.

Other Concerns

Stakeholders report considerable concern that China's rules and procedures limit parties' abilities to challenge GI's via opposition, cancellation, invalidation, and other processes that would ensure GIs do not impose market access barriers to U.S. exports. In 2014 and 2015, the United States welcomed important Chinese commitments on rules and procedures concerning the registration of GIs under China's existing systems, as well as those registered pursuant to an international

agreement. In late February 2019, CNIPA issued for comment draft revisions to the Measure on Protection of Foreign Geographical Indication Products. In detailed comments on the draft, the United States explained that it is critical that the final version of the revisions ensure full transparency and procedural fairness with respect to the protection of GIs, including safeguards for generic terms, respect for prior trademark rights, clear procedures to allow for opposition and cancellation, and fair market access for U.S. exports to China relying on trademarks or the use of generic terms.

The United States continues to urge all levels of the Chinese government, as well as state-owned enterprises (SOEs), to use only legitimate, licensed copies of software. Right holders report that government and SOE software legalization programs still are not implemented comprehensively and urge the use of external audits to ensure accountability. Though it reflects a slight decline from past years, the reported 66 percent rate of unlicensed software use in China represents $6.8 billion in lost commercial value, far above regional and global rates.

Finally, stakeholders have identified concerns relating to opposition examiners at the China Trademark Office, who face very large dockets and whose decisions on likelihood of confusion are often narrowly focused on goods or services in the same sub-class rather than also taking into account goods and services in other classes and other market realities. Stakeholders continue to report that trademark authorities do not give full consideration to co-existence agreements and letters of consent in registration processes, among other issues. Additional concerns include onerous documentation requirements for opposition, cancellation, and invalidation proceedings, lack of transparency in opposition proceedings, absence of default judgments against applicants who fail to appear, and legitimate right holders' difficulty in obtaining well-known trademark status. Moreover, changes to trademark opposition procedures eliminated appeals for opposers, which resulted in longer windows for bad-faith trademark registrants to use their marks—or blackmail the legitimate brand owner—before a decision is made in an invalidation proceeding.

EXHIBIT 13

TECH

THE PULSE @ 1 MARKET

THE PULSE @ 1 MARKET

How Amazon counterfeits put this man's business on brink of collapse

PUBLISHED MON, OCT 24 2016•10:00 AM EDT UPDATED MON, OCT 24 2016•11:42 AM EDT

Ari Levy
@LEVYNEWS

SHARE

Production line of the Forearm Forklift

Jeniece Pettitt | CNBC

Counterfeiters on Amazon are killing this small business

Mark Lopreiato was thrilled when he was invited to promote his Forearm Forklift on ABC's "Good Morning America" last month. The chance for a small manufacturing business to reach 4.5 million viewers for free doesn't come around often.

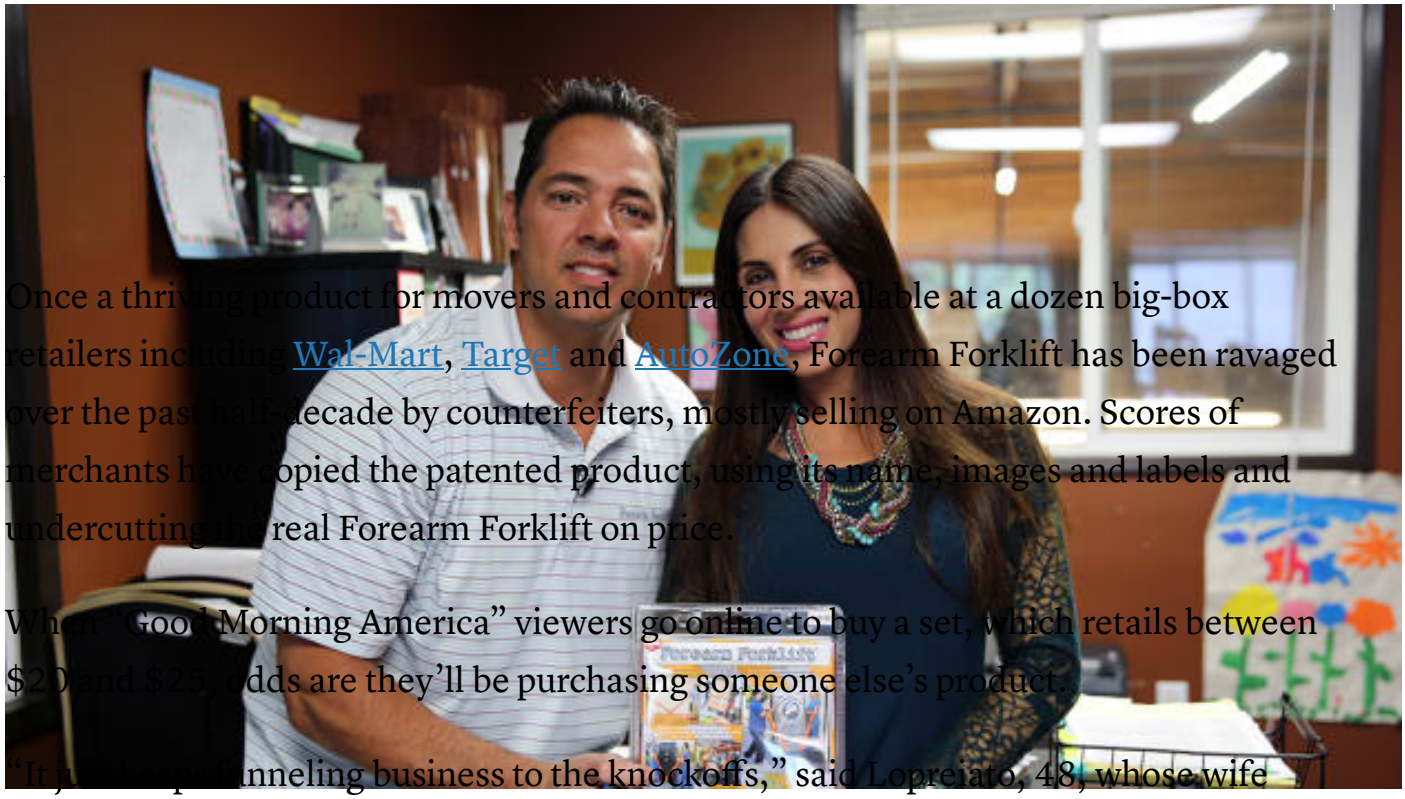
Lopreiato appeared on "Buy it and Try It," a segment for hosts to test out popular niche gizmos from infomercials in front of an enthusiastic New York studio audience. The first product they tried was a steel nonstick pan, which smoothly cooked up eggs without the use of oil or butter.

Then it was Forearm Forklift's turn. After viewing a commercial for the product, ABC's Lara Spencer and Gio Benitez pulled the heavy-duty moving straps over their forearms and proceeded to lift up a washing machine and walk with it.

"I was pretty impressed," Spencer said to the crowd.

You'd think such a shout-out from the hugely popular morning show would provide a huge boost for Lopreiato's 18-year-old family business.

But this is Amazon.com's world, and Forearm Forklift, like so many brands, is uncomfortably inhabiting it.



Once a thriving product for movers and contractors available at a dozen big-box retailers including Wal-Mart, Target and AutoZone, Forearm Forklift has been ravaged over the past half-decade by counterfeiters, mostly selling on Amazon. Scores of merchants have copied the patented product, using its name, images and labels and undercutting the real Forearm Forklift on price.

When "Good Morning America" viewers go online to buy a set, which retails between $20 and $25, odds are they'll be purchasing someone else's product.

"It just keeps funneling business to the knockoffs," said Lopreiato, 48, whose wife Sophia also works at the company and traveled with him to New York. "It's almost like winning the lottery if they choose our item."

Forearm Forklift is hanging on by a thread. The company is down to 21 full-time employees from 52 at its peak and recorded less than $500 in profit last year. Annual revenue in 2008 topped $4 million and has since plunged 30 percent. Retailers stopped placing orders because they were finding what appeared to be the same thing online for much cheaper.

Lopreiato has diversified his product line, adding a harness for the shoulders, a strap that goes over a single shoulder and straps for carrying boxes. But nothing has come close to replicating the success of his flagship Forearm Forklift.

Meanwhile, Lopreiato bears the costs of workers' compensation, product quality control, commercial insurance, mortgage payments and patent management fees all so counterfeiters can act as freeloaders.

Amazon price targets

"We're competing with people who are stealing our brand, stealing our pictures and

20,000-square foot warehouse in Baldwin Park, about 20 miles east of Los Angeles.

Amazon's growing dominance in commerce brings with it plenty of collateral damage. The counterfeit problem, in particular, goes largely undiscussed by CEO Jeff Bezos and ignored by investors and analysts.

The stock has climbed 37 percent over the last 12 months making Amazon the world's fourth-most valuable company, and 89 percent of analysts tracked by FactSet say shareholders should buy more.

Heading into the Seattle-based company's third-quarter earnings report Thursday, investor focus is on Amazon Web Services, Prime membership growth and additional investments in supply chain and fulfillment. Analysts at Pacific Crest Securities, in their earnings preview, called Amazon "one of the most disruptive forces in retail and technology today."

Conversations with merchants elicit a very different reaction. Since CNBC.com began reporting on Amazon's budding counterfeit issue in May, we've spoken with dozens of merchants that have narratives similar to Lopreiato's, but very few are willing to speak on the record out of fear of retribution from Amazon.

Lopreiato, an Army veteran and father of two middle-school daughters, said he felt compelled to tell his story.

"If Jeff Bezos knew exactly what was happening to us, he'd do the right thing," he said. "It's not that he's a bad guy. It's that there is, in my opinion, a lot of pressure put on folks at Amazon to increase sales, increase sales, increase sales. That's wonderful. That's the American way. But do it right."

Jeff Bezos
Brent Lewis | The Denver Post | Getty Images

Amazon's obsessive focus on pleasing consumers with discounts and service has come at the expense of brands like Forearm Forklift. In trying to provide the lowest-cost option for virtually every product on the planet, the company opened the doors to merchants from across the globe with little respect for intellectual property, despite an anti-counterfeiting policy that prohibits the sale of inauthentic items.

That's enabled manufacturers largely from China to take advantage of cheaper production and labor costs to compete on the Amazon market.

Some big brands have voiced their concerns.

Birkenstock said in July that it's no longer authorizing sales on Amazon starting in 2017. Last week Apple sued a distributor named Mobile Star for selling counterfeit power adapters and charging cables on the site, claiming the products "pose an immediate threat to consumer safety."

Amazon has taken steps to crack down of late by forcing new sellers of major brands like Nike, Hasbro and Cuisinart to show invoices proving the items are legitimate and then pay a fee. Third-party sellers are getting suspended in droves for activity that Amazon deems suspicious or for complaints from buyers, sparking outrage from merchants who say they're being punished for Amazon's inability to control counterfeiting.

"Amazon has zero tolerance for the sale of counterfeits," a company spokesperson said in an e-mailed statement. "We are working closely with manufacturers and brands to

identify offenders, and removing fraudulent items from our catalog. We are also taking action and aggressively pursuing bad actors in this space."

The company didn't offer a comment on Forearm Forklift's situation.

Until now, Forearm Forklift has been forced to self-police the site and take action to get unauthorized listings removed. See an infringer? Send a cease-and-desist letter. Suspicious of a counterfeit? Buy it, and prove to Amazon through a formal complaint that the listing should be taken down.

Repeat, repeat, repeat. And pray it works.

Jeniece Pettitt | CNBC

On the second floor of Forearm Forklift's warehouse, Lopreiato opens a closet filled floor-to-ceiling with cardboard boxes from Amazon purchases. Inside each, supposedly, is a version of his product.

There's no subtlety. The packaging includes not only his name and label but images of

equipment. Open a box and find orange straps that are either too thin, too short, have loose stitching or are made of entirely different and weaker material.

Lopreiato said he's submitted more than 100 cease-and-desist letters to third-party sellers and takedown notices to Amazon. But go to Amazon today, and infringers are easy to spot. One listing for furniture moving straps contains an image that looks like a couple of seat belts. Among the attached photos is one of Mark's wife moving a mattress.

In a July 2015 e-mail to Amazon's patent team, Marty Proops, an Amazon marketplace expert who previously worked with Forearm Forklift on its account, said he and Lopreiato had identified 53 separate sellers offering infringing products over the past year.

Buyers who assume they're getting the real thing are dismayed when the product can't possibly help them move a 300-pound refrigerator. Thus, Forearm Forklift has one-star reviews from customers calling it a "cheap knockoff (don't purchase)" and "very obvious counterfeit."

"That posts on our offer page on Amazon so a lot of people think we're offering fakes," Lopreiato said.

He never expected this to be easy. He developed the original contraption while working as a mover and dealing with clients who didn't want dollies rolling across new wooden floors. Carrying items by hand meant bending down with 200-pound appliances to get through doorways.

Lopreiato got started renting a small warehouse in 1998 and had so little money that he lived in the office. He had an evening gig at a law firm doing clerical work and waited tables on weekends.

For 12 years, Lopreiato built the business by attending trade shows and networking with distributors and buyers. He forged deals with companies ranging from U-Haul and Home Depot to Ross Stores and Canadian Tire.

He was on QVC every two months or so starting in 2003, selling more than 20,000 Forearm Forklifts per live show at the peak. He started selling to Amazon as a vendor that same year, but it was never a big part of his business, representing under 2 percent of revenue in 2008.

Lopreiato was fully prepared for competition, knowing that patent protection only goes so far. But he never expected a counterfeiting onslaught.

The slide started in 2010. He got a call from an Amazon employee, saying that other sellers were offering his product at a much lower price and he needed to cut his rate to keep the business.

Lopreiato investigated and quickly found the rival products were fakes. He told Amazon that he would aggressively defend his intellectual property but that he couldn't compete with those prices and still make money. Amazon was unhappy with that response, and within weeks there were more than 100 knockoffs on the site, Lopreiato said.

"Since that date, it's just been absolutely downhill," he said.

Over the past six years, Lopreiato has seen vendor managers come and go without fixing the problem or notifying him that they're leaving.

He forwarded a number of e-mails from the past two years, where he and Proops showed explicit infringement and asked for help. In addition to jeopardizing Forearm Forklift's business, Proops wrote in June 2015, "Sooner or later an Amazon customer is going to be seriously injured by one of these cheap knockoffs!"

Responses ranged from terse to deflecting. Amazon told Proops to send complaints to generic e-mail addresses copyright@amazon.com and patents@amazon.com. Other e-mails suggested that the company was looking into the matter, but then the account would move to another representative.

In July 2015, an Amazon lawyer told Proops by e-mail that Forearm Forklift should take up infringement matters directly with the third-party sellers. "At this time we consider this matter closed and we will take no further action," he wrote.

C.J. Rosenbaum, a lawyer who represents Amazon sellers, said the rapid turnover in vendor managers and inconsistency in how they treat issues is a constant source of frustration.

"Amazon's responses are very erratic," said Rosenbaum, who recently published the "Amazon Law Library," a book compiling the legal issues surrounding the company and platform. "You can send in one complaint through the system about an IP violation and they take down the listing, and submit the same exact thing again and just fail."

Forearm Forklift
Jeniece Pettitt | CNBC

For Lopreiato, legal action presents an expensive option with little upside. Individually going after infringers, who he'd first have to track down, would require more time and money than he's got in the bank. He filed one case in 2013 against a domestic company and was awarded a settlement before trial.

Taking on Amazon directly has been a nonstarter for the three intellectual property lawyers Lopreiato has contacted.

More than anything, he needs Amazon's help. With traditional retailers sinking fast and more retail and wholesale activity shifting to Amazon, Forearm Forklift now counts on the site for about 12 percent of revenue, a number that's growing despite the flood of counterfeits.

A tiny number of additional orders rolled in after the "Good Morning America" appearance, even though Lopreiato is certain that far more went to the knockoffs.

Similarly, a Facebook page called Impressive Things posted Forearm Forklift's commercial earlier this month, generating 909,000 views and counting. Again, more revenue for the fakes.

On Friday morning, Lopreiato received a particularly discouraging call.

Aafes, a retailer targeting military communities, had been planning to buy Forearm Forklift for 120 of its stores. The representative handling the deal was calling Lopreiato because an Aafes executive had discovered lookalikes on Amazon for a much lower

He e-mailed a screenshot showing two different sellers using Forearm Forklift's photos (including the one below) to promote their products, one for $8.09 and the other for $11.24.

Lopreiato is all too familiar with this routine. He replied with a lengthy apology and offered assurance that the cheaper products are fakes. He gave his standard "buyer beware" pitch, explaining that the knockoffs are low quality, unsafe and uninsured.

He's not at all confident that it will be enough. In a text message on Friday afternoon, Lopreiato wrote, "Another prospect will probably be lost."

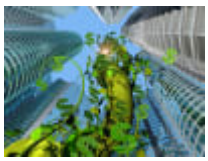
RELATED

This hot robot says she wants to destroy humans

Birkenstock quits Amazon in US after surge in counterfeit sales

Hit men, drugs and malicious teens: the darknet is going mainstream

Prepare for hackers to change your credit score



How to buy into start-up growth, with less risk

MORE IN THE PULSE @ 1 MARKET

Uber’s making a big bet on business travel

Deirdre Bosa

Bringing back jobs means using artificial intelligence to stay competitive, executive says

Anita Balakrishnan

Riding Salesforce and Amazon’s cloud to $1 billion

Ari Levy

READ MORE

Subscribe to CNBC PRO
CNBC Councils
Advertise With Us
Digital Products
Closed Captioning
About CNBC
Site Map
AdChoices
Help

Licensing & Reprints
Supply Chain Values
Join the CNBC Panel
News Releases
Corrections
Internships
Podcasts
Careers
Contact

News Tips
Got a confidential news tip? We want to hear from you.

GET IN TOUCH

CNBC Newsletters
Sign up for free newsletters and get more CNBC delivered to your inbox

SIGN UP NOW

Get this delivered to your inbox, and more info about our products and services.

Privacy Policy
Do Not Sell My Personal Information

© 2020 CNBC LLC. All Rights Reserved. A Division of NBCUniversal

Data is a real-time snapshot *Data is delayed at least 15 minutes. Global Business and Financial News, Stock Quotes, and Market Data and Analysis.

Market Data Terms of Use and Disclaimers

Data also provided by

EXHIBIT 14

U.S. pet ownership statistics

Companion animals | Exotic animals | Formulas/Calculator

Source: *2017-2018 U.S. Pet Ownership & Demographics Sourcebook*

Companion animals

	Dogs	Cats	Birds	Horses
Percent of households owning	38.4	25.4	2.8	0.7
Number of households owning	48,255,413	31,896,077	3,509,032	893,152
Average number owned per household	1.6	1.8	2.1	2.1
Total number in United States	76,811,305	58,385,725	7,538,000	1,914,394
Veterinary visits per household per year (mean)	2.4	1.3	0.3	1.6
Veterinary expenditure per household per year (mean)	$410	$182	$40	$614
Veterinary expenditure per animal (mean)	$253	$98	$18	$291

View 2012 statistics

Specialty and Exotic Animals

	Households (in 1,000)	Population (in 1,000)
Fish	10,475	76,323
Ferrets	326	501
Rabbits	1,534	2,244