AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–577

PROTECTING E-COMMERCE CONSUMERS FROM COUNTERFEITS

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MARCH 6, 2018

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE
35–965—PDF WASHINGTON : 2019

COMMITTEE ON FINANCE

ORRIN G. HATCH, Utah, *Chairman*

CHUCK GRASSLEY, Iowa
MIKE CRAPO, Idaho
PAT ROBERTS, Kansas
MICHAEL B. ENZI, Wyoming
JOHN CORNYN, Texas
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina
JOHNNY ISAKSON, Georgia
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania
DEAN HELLER, Nevada
TIM SCOTT, South Carolina
BILL CASSIDY, Louisiana

RON WYDEN, Oregon
DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
BILL NELSON, Florida
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, JR., Pennsylvania
MARK R. WARNER, Virginia
CLAIRE MCCASKILL, Missouri
SHELDON WHITEHOUSE, Rhode Island

A. JAY KHOSLA, *Staff Director*
JOSHUA SHEINKMAN, *Democratic Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Hatch, Hon. Orrin G., a U.S. Senator from Utah, chairman, Committee on Finance	1
Wyden, Hon. Ron, a U.S. Senator from Oregon	4

WITNESSES

Gianopoulos, Kimberly, Director, International Affairs and Trade, Government Accountability Office, Washington, DC	7
Smith, Brenda, Executive Assistant Commissioner, Office of Trade, Customs and Border Protection, Washington, DC	9
Joholske, Jim, Director, Office of Import Surveillance, Consumer Product Safety Commission, Washington, DC	11
Brady, Terrence R., president, Underwriters Laboratories, Inc., Northbrook, IL	12

ALPHABETICAL LISTING AND APPENDIX MATERIAL

Brady, Terrence R.:	
Testimony	12
Prepared statement	25
Gianopoulos, Kimberly:	
Testimony	7
Prepared statement	27
Responses to questions from committee members	32
Hatch, Hon. Orrin G.:	
Opening statement	1
Prepared statement with attachments	37
Joholske, Jim:	
Testimony	11
Prepared statement	47
Responses to questions from committee members	48
Smith, Brenda:	
Testimony	9
Prepared statement	52
Responses to questions from committee members	58
Wyden, Hon. Ron:	
Opening statement	4
Prepared statement	75

COMMUNICATIONS

Alliance for Safe Online Pharmacies	77
Asmodee North America, Inc.	79
Coalition to Combat Counterfeiting (CCC)	88
The Counterfeit Report	90
Precious Metals Association of North America	93

PROTECTING E-COMMERCE CONSUMERS FROM COUNTERFEITS

TUESDAY, MARCH 6, 2018

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:03 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Orrin G. Hatch (chairman of the committee) presiding.

Present: Senators Thune, Isakson, Portman, Heller, Cassidy, Wyden, Stabenow, Cantwell, Menendez, Carper, Cardin, Bennet, Casey, Warner, and McCaskill.

Also present: Republican staff: Christopher Armstrong, Chief Oversight Counsel; Joshua Blume, Professional Staff Member; and Queena Fan, Detailee. Democratic staff: Elissa Alben, International Trade Counsel; David Berick, Chief Investigator; Daniel Goshorn, Investigative Counsel; Greta Peisch, International Trade Counsel; and Jayme White, Chief Advisor for International Competitiveness and Innovation.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM UTAH, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. This hearing will come to order.

I would like to welcome everyone here today. During this hearing, we will discuss counterfeiting and e-commerce and what steps we can take to protect consumers.

Before we get to that, though, I would like to make an important point about the President's proposed tariffs on steel and aluminum.

Let us set aside just for a moment all of the legitimate concerns about trade wars, the failure to target the source of steel and aluminum overcapacity, and the disproportionate effects on our major trading partners and allies.

In the end, these tariffs are not a tax on foreign steel and aluminum producers, but rather a tax on American citizens and businesses who, if this action is finalized, will be forced to pay an additional 25 percent on steel and 10 percent on aluminum.

Those effects would blunt the benefits of tax reform for all Americans, including the reduced impact of billions of dollars that many companies recently pledged to invest here in America. And those billions will not be as valuable. Truly, there is a better way to address China's actions than to impose a new, across-the-board tax on U.S. consumers and businesses just 3 short months after we passed comprehensive tax reform.

We can and we should do better. And I will be sending the President a letter later today emphasizing just that.

Now, I would like to turn to the important issues we want to address in this hearing. It is no secret that I have long felt, and I think others feel the same way, that strong protections for intellectual property rights protect consumers. A properly enforced trademark, for example, lets a customer know who made a product and where to go for information about it.

We were all encouraged by the new authorities the Trade Facilitation and Trade Enforcement Act of 2015 granted the U.S. Customs and Border Protection as well as Immigration and Customs Enforcement. Those authorities along with a new National Intellectual Property Center were designed to help agencies collaborate, coordinate, and take down perpetrators.

And because there are frequently hiccups with the implementation of new laws, the committee asked the Government Accountability Office to conduct a broad investigation about how the Trade Facilitation and Trade Enforcement Act was being implemented.

As they started their investigation, GAO quickly began to realize that e-commerce generally was causing major issues for CBP and ICE. Due to advancements in online purchasing, the agencies were being forced to adopt new tactics, work more closely together, and build up their public/private partnerships. Those have all been changes for the good.

However, we asked GAO to continue their investigation and to look specifically at the problem of counterfeits on some of the most prominent e-commerce platforms. As part of this process, GAO made purchases from five major e-commerce platforms, and, after using relatively narrow criteria, GAO received at least one counterfeit and one legitimate good from each of the platforms.

In the end, 20 of the 47 individual items they purchased were counterfeit. While the sample size was small, the results are still telling.

On the whole, this investigation started us down a path of discovery. And on that path, we noticed that there are far more issues than we had initially anticipated.

Today's hearing represents a combination of those initial findings. And while we are not going to be able to fix this all at once, I am hoping to at least discuss some of the meaningful steps that we could take in the near term. But before we get to that, I want to talk a little bit more about what we found as part of this research.

As part of its research, GAO found that many counterfeit products create a hazard to consumers, children, and our economy. Through seizures and later investigations, CBP, ICE, and CPSC have found numerous instances of counterfeit products with major health and safety issues. These issues have included contact lenses that contain dangerous bacteria, cosmetics that have chemicals that can cause harmful health effects when applied, phone chargers with faulty wiring, batteries with thermal runoff issues, and even defective airbags.

GAO has found that with the rise of popular online marketplaces, counterfeiters have greater access to the market and can easily sell their phony products directly to consumers.

Because the counterfeiters frequently use stock photos or simply join in on a prelisted product, the goods are sold as genuine. And so long as counterfeiters can make the products indistinguishable on the outside, most consumers have never noticed a difference. This is because typical red flags for consumers are difficult to notice.

This is even true when the counterfeiters create new colors or designs of more famous products. In one recent instance, the U.S. Attorneys Office in the Northern District of Mississippi successfully prosecuted a case against Bobby Rodgers, Jr.

Mr. Rodgers had a fairly elaborate scheme in place. First, he would order counterfeit merchandise from China and facilitate delivery by using alternate addresses. Then he would powder-coat the counterfeit items he received and sell them as a third-party retailer online. As he did this, he would represent the goods as authentic, sometimes even with licensed modifications.

The sheer volume of his scams was staggering. On just one of the two major platforms that he used, Mr. Rodgers had sold over $300,000 in counterfeit goods.

When his complex was raided, authorities seized another 2,200 pieces of counterfeit drinkware. But it does not end there.

Later, as the CPSC lab reports came back, several of the colors tested positively for lead, exceeding the amount legally allowed by more than 20 times. For all we know, there are currently children around the country sipping water with dangerously high levels of lead because of Mr. Rodgers.

Sadly, he is just one among many, many perpetrators buying counterfeits and facilitating sales of them through e-commerce platforms.

We have heard from some rights holders, like YETI, whose products have been counterfeited in these schemes, who have responded strongly to address these problems. YETI issued a statement making it clear that they were expending, quote, "significant resources to protect [their] consumers," unquote.

I ask unanimous consent that the full YETI statement, as well similar statements submitted by other rights holders, be entered into the appropriate place in this hearing record.

[The statements appear in the appendix beginning on p. 39.]

The CHAIRMAN. Now, I do not want to steal too much of their thunder, but one of the reasons we have invited Underwriters Laboratories, or UL, here today is to let them give us a broader perspective on the seriousness of these issues.

As just one example, in a public report, UL recently tested 400 counterfeit Apple phone adapters. Out of those 400, they found that only three out of the 400 chargers passed electricity strength tests. And that is just one of the many studies UL has performed.

I think everyone here, both members and the audience, will be stunned by not only the breadth of products being counterfeited, but also by the incredible volume. This goes beyond the dollars and cents these companies have invested to develop and market their products, which, let us be clear, are enormously important for our economy, not to mention the well-being of American consumers.

But we are not just talking about devalued investments. We are talking about lead on children's drinkware, phones catching fire,

homes burning down, consumers being injured from hygiene and cosmetic products, airbags not inflating properly, and who knows what else.

It is my hope that we all can agree today that counterfeit products pose an immediate and significant risk to Americans' health and safety. And I hope that we can take GAO's recommendations seriously to improve information sharing and better track CBP's intellectual property enforcement methods.

Personally, I am interested in talking specifically about sharing e-commerce platform data contained in invoices and on packages with rights holders, as well as learning from and improving CBP's voluntary abandonment program.

American consumers are relying on us to get this right, and we need to work together and with the appropriate officers at CBP, ICE, and other agencies to make sure we do.

With that, I am very happy to turn to my colleague and partner, Senator Wyden, for his opening remarks.

[The prepared statement of Chairman Hatch appears in the appendix.]

OPENING STATEMENT OF HON. RON WYDEN, A U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you very much, Mr. Chairman.

Mr. Chairman, you commented on the steel and aluminum issue, and I would like to start with some brief comments on that as well.

The fact is, on the steel and aluminum issue, the President has inflicted a punishing year of uncertainty on the American economy. And this uncertainty has harmed our workers, American workers who need and deserve good-paying jobs.

Moreover, even as of this morning, it is still not clear that the President understands the central problem, which is dealing with Chinese overcapacity of steel.

So he has had practically one salvo a day with respect to trade. One day he is looking at tariffs, the next day he is looking at in some way intertwining his steel policy with the North American Free Trade Agreement.

I just want it understood that this year of uncertainty, which already caused an import surge when the President basically dawdled right out of the gate, has real consequences for American workers and American families, and they deserve better.

Now, with respect to this hearing, the committee will be discussing the challenge of protecting consumers from counterfeit goods. And I am glad that this discussion is taking place. It is long overdue.

I also hope this committee will soon hold hearings on the Trump administration's varied and sundry trade activities, including the steel and aluminum investigations and potential tariffs, the North America Free Trade Act renegotiations, and the investigation of China under section 301.

On counterfeit imports, any discussion of this issue has to begin by recognizing that over the last few decades, the Internet has transformed virtually every corner of the American economy.

I stated some time ago in this room that the Internet is now the shipping lane of the 21st century. And that is a far cry from the kind of trade discussions that took place for decades in this room.

People now take it for granted, but it is, in effect, a miracle of modern commerce that a small business in my home State of Oregon, 3,000 miles from Washington, DC, can reach consumers almost anywhere at any time. No longer does expanding your customer base mean investing solely in bricks and mortar.

Wildfang is a socially conscious Portland clothing company that was founded by women and run by women. They have two stores in Portland, but what is really driving sales is online opportunities, online sales. A full 70 percent of their business happens online, and that is where we are seeing the growth. This is a company that has seized the opportunity to sell around the world via the Internet, and it now has 25 employees.

But the fact is, anytime there is significant economic change, let alone the kind of transformative activity that the Internet has brought, you get some new challenges along with the upside. That includes the chance that when you buy something online, there is a chance it could be a fake.

It is up to the Federal Government to make sure our approach to combating counterfeits is not stuck in the 20th century.

These days, when you talk about cracking down on counterfeit goods, you are no longer talking about stopping the person selling fake purses out of their trunk. You are talking about illegitimate products passed off on even the most savvy, streetwise consumers, and often they are mixed right in with the genuine products that our people want.

Many of those fakes pose serious dangers. Makeup and food and beverage containers can be made with dangerous chemicals. Electronics can pose a fire hazard. There can be toys that are unsafe for kids.

The number of small packages coming into America has surged, and the fact is that Customs and Border Protection has to step up and play a major role in identifying counterfeits and stopping them before they enter the marketplace. Unfortunately, so far, we get a sense that Customs and Border Protection is just too often playing catch-up ball tracking these fake products down.

After conducting a recent study of this exact issue, the Government Accountability Office recommended a set of policy updates to have Customs and Border Protection work more closely with the private sector. Those recommendations include expanding Customs and Border Protection authority to notify online sales platforms when they have products on their hands that might be fake.

Now, you may hope that that would set the wheels in motion and this would result in the policies being in place. But Customs and Border Protection has responded to this audit by claiming it would take until this upcoming September to determine if additional authority was actually necessary.

Over the last few years, the committee has put a lot of sweat equity into the policies that have strengthened the enforcement of our trade laws and have done more to protect the American consumer and the American worker.

The chairman and I authored the Trade Facilitation and Trade Enforcement Act of 2015 that put in place important new tools for Customs and Border Protection to detect and prevent counterfeits, including sharing information about counterfeit imports with rights holders.

So in preparation for the hearing, committee staff from both sides sat down with Customs to dig into the issue.

My staff asked, and I quote here, "Does Customs and Border Protection need more authority to crack down on the rip-off artists and the counterfeiters?" The agency said they do not know.

When asked when they would know, they said they did not know when they might know.

So as we begin this hearing, it certainly is unsettling that it has not been possible for the Finance Committee on a bipartisan basis to get a straight answer on a matter like this from the agency that is central to America's effort to protect our consumers from counterfeit goods.

So this morning, I am going to give the agency one more try to answer those questions.

Let me close by saying, getting this right is not going to be as simple as just putting a few more policy tools in the agency's kit.

Year after year, administrations have fallen short in hiring enough officers—blue uniforms—to fulfill the critical need of protecting our consumers and businesses from illegal and unfairly traded goods.

This agency has a tough job working with other law enforcement agencies and foreign governments to go after the source of the problems. If the administration is focused solely on hiring an army of Border Patrol agents, I do not see how that is going to help them build their capacity to deal with the counterfeit challenges.

So the Congress and the administration need to ensure that the agency has the resources it needs to combat counterfeiters and that there is actual follow-up.

This is simply a matter of protecting American families from harmful products and making sure that we are fully mobilized to stop these rip-off artists from undercutting the American brand. That is really their objective, to undercut the American brand. So getting this right to reflect the realities of the modern economy is, in my view, what this hearing is all about.

And, Mr. Chairman, as usual, I look forward to working with you.

The CHAIRMAN. Well, thank you, Senator.

[The prepared statement of Senator Wyden appears in the appendix.]

The CHAIRMAN. I would like to extend, both of us would like to extend a warm welcome to each of our four witnesses today. I want to thank you all for coming.

First, we will hear from Ms. Kimberly Gianopoulos, Director for International Trade Issues in the International Affairs and Trade team at the Government Accountability Office.

Ms. Gianopoulos has received a number of awards, including the Meritorious Service Award, a Client Service Award, an Assistant Comptroller General's Award, and several Results Through Teamwork Awards. She is also a certified government financial manager.

Ms. Gianopoulos earned a bachelor's degree in mathematics and a master's degree in public analysis and administration from the State University of New York at Binghamton.

The second witness on our panel is Ms. Brenda Smith, Executive Assistant Commissioner, Office of Trade, U.S. Customs and Border Protection. Ms. Smith has overseen her office since 2014 and has been with CBP since 1994.

Prior to joining Customs, Ms. Smith worked at the Department of the Treasury and on Capitol Hill. She was honored in 2017 with the Distinguished Executive Presidential Rank Award, the highest award in civil service.

Ms. Smith holds bachelor's and master's degrees in economics from Rutgers University and is also a graduate of the Customs Leadership Institute and the Federal Executive Institute.

Next to speak will be Mr. Jim Joholske, Director for the Office of Import Surveillance at the U.S. Consumer Product Safety Commission.

Mr. Joholske started his career at CPSC in July 2000 with the agency's Office of Compliance and Field Operations. At that time, he focused primarily on enforcement of regulations regarding fireworks and cigarette lighters.

Jim later joined Import Surveillance in 2008 and served as Deputy Director prior to assuming the role of Director in March 2017.

Finally, Mr. Terrence R. Brady, the president of Underwriters Laboratories, Inc., will testify. Mr. Brady was appointed to his new position just last week, but was just recently serving UL as a vice president and chief commercial and legal officer.

Prior to joining UL, Mr. Brady was an associate and partner for 27 years in the Chicago office of Winston and Strawn, LLP.

Mr. Brady graduated from Dartmouth College with his undergraduate degree and then received his law degree from Notre Dame Law School.

I want to thank you all for coming and being here with us today and for testifying today.

So, Ms. Gianopoulos, we will turn to you first, and we will begin with your opening remarks.

STATEMENT OF KIMBERLY GIANOPOULOS, DIRECTOR, INTERNATIONAL AFFAIRS AND TRADE, GOVERNMENT ACCOUNTABILITY OFFICE, WASHINGTON, DC

Ms. GIANOPOULOS. Thank you, Mr. Chairman.

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to be here today to discuss our recent work on intellectual property rights.

The United States is a global leader in the creation of intellectual property. Companies that illegally import and distribute counterfeit goods can cause a number of harmful effects on the U.S. economy, such as slowing economic growth and threatening American jobs. What is more, the counterfeit goods could threaten the health and safety of the American people.

My testimony today summarizes the findings from our recent report and covers three main areas. First, I will talk about some of the difficulties that are presented by counterfeit goods in e-commerce, using information from our investigation to illustrate just

how challenging that problem is. Second, I will discuss the nature of efforts that Customs and Border Protection and Immigration and Customs Enforcement have undertaken to enhance IPR enforcement. And finally, I will cover some of the ways in which CBP and ICE coordinate with the private sector in enforcing IPR.

The rise of e-commerce has contributed to a fundamental change in the market for counterfeit goods. In the past, you may have expected to find counterfeit purses or watches on a street corner or in a flea market. These goods may have been shipped to the United States on a cargo ship in bulk and were priced significantly below retail.

Now many people shop online, where sellers of counterfeit goods engage in a number of practices to make their goods look authentic. Numerous, everyday items can be counterfeit. This practice is no longer limited to high-end goods.

These online purchases are sent to buyers in individual express packages rather than shipped in bulk to U.S.-based distributors. This makes it very challenging for consumers as well as CBP to identify counterfeit goods.

As part of our review, we purchased 47 items covering four different types of consumer goods, including Nike Air Jordan shoes, YETI travel mugs, Urban Decay cosmetics, and UL-certified phone chargers, from five different popular e-commerce websites.

We looked for items that were advertised as new, brand-name items and were sold by highly rated third-party sellers. Of the 47 items, 20 were counterfeit as determined by the rights holders themselves.

It can be difficult to tell if an item is counterfeit. For example, these are three of the YETI mugs that we purchased online. These two silver mugs look identical, they feel the same, same weight. But if you look at the bottom, you will see that one of them has misspellings on the words. For example, Austin, TX as the source is spelled A-U-S-I-N and it says "mede" in China instead of made in China.

And then this hot-pink mug also seems to be authentic, except, well, YETI does not make hot-pink mugs. So you would not know that unless you were aware of that issue with regard to YETI.

In our full report, we include a one-page appendix that lists a number of ways consumers can take steps to avoid purchasing counterfeits online.

To enhance IPR enforcement, we found that CBP and ICE engage in a number of activities. They conduct special operations at U.S. ports, engage with international partners, and undertake localized programs or port-led initiatives.

However, CBP has conducted a limited amount of evaluation of its efforts and may, therefore, not have the information it needs to be as effective and as efficient as possible given our current resource-constrained environment.

We recommended that CBP take steps to evaluate the effectiveness of its IPR enforcement efforts. And the agency agreed with our recommendation.

With regard to the private sector, we found that CBP is restricted in the amount and type of information about seized items

that it can share. This restriction limits the ability of rights holders and e-commerce websites to protect IPR.

In the Trade Facilitation and Trade Enforcement Act of 2015, Congress gave CBP authority to share certain information with trademark and copyright owners before completing a seizure. However, CBP officials told us that there are legal limitations to this sharing. For example, CBP cannot share information from the exterior of seized packages. This could help websites identify groups of counterfeit merchandise from the same seller.

We recommended that CBP assess what information would be helpful to share with the private sector and take appropriate action to enhance information sharing where possible. And CBP agreed with this recommendation.

This concludes my opening remarks. Thank you for your time, and I am happy to answer any questions you might have.

The CHAIRMAN. Thank you very much.

[The prepared statement of Ms. Gianopoulos appears in the appendix.]

The CHAIRMAN. Ms. Smith, we will turn to you.

STATEMENT OF BRENDA SMITH, EXECUTIVE ASSISTANT COMMISSIONER, OFFICE OF TRADE, CUSTOMS AND BORDER PROTECTION, WASHINGTON, DC

Ms. SMITH. Chairman Hatch, Ranking Member Wyden, and distinguished members of the committee, it is an honor to appear today to discuss CBP's enforcement of intellectual property rights and our efforts to keep counterfeit goods that pose a threat to the health and safety of American consumers from entering U.S. commerce.

As America's unified border agency, CBP enforces nearly 500 U.S. trade laws and regulations on behalf of 48 Federal agencies. This morning, I would like to give you my perspective of the opportunities and challenges we see in the current trade environment.

Thanks to this committee's support and commitment, the Trade Facilitation and Trade Enforcement Act of 2015 strengthened and expanded CBP's authority to enforce our Nation's trade laws, while facilitating lawful international trade.

Among its many provisions, the Trade Facilitation and Trade Enforcement Act, also known as TFTEA, provided significant cost-savings opportunities for U.S. businesses and consumers by raising the *de minimis* threshold from $200 to $800, which allows relatively low-value goods to be brought into the United States free of duty and with reduced information requirements.

The combination of growing online purchases and the higher threshold has resulted in increasing U.S. imports of small, just-in-time packages, many arriving via international mail and express consignment carriers.

Over the past 5 years, the volume of international air-express shipments has increased nearly 50 percent, and in the postal environment, small packages have increased by over 200 percent. This rise in small packages has altered the dynamic of the trade environment and CBP's ability to enforce intellectual property rights.

CBP targets for a variety of risks and takes action when it finds a problem. In fiscal year 2017, CBP seized over 34,000 shipments

of counterfeit goods, an 8-percent increase over the previous year and very consistent with the trend that we have seen over the last 10 years.

Approximately 16 percent of these seized goods, such as cosmetics, electronics, and toys, contain serious potential threats to consumer health and safety.

We are currently enforcing more than 18,000 copyright and trademark records. Rights holder collaboration through recordation, training, and the information sharing strengthened by TFTEA is essential to identifying counterfeit products.

CBP also regularly discloses information to the rights holders to verify a product's validity if we suspect that imported merchandise bears a counterfeit mark.

This private-sector partnership, as envisioned by TFTEA, is continuing to expand with the recent announcement of the first partnership arrangement under the IPR Enforcement Donations Acceptance Program in which Procter and Gamble has donated testing devices to help CBP quickly determine the authenticity of its product.

Interagency partnership is supported through the Commercial Targeting and Analysis Center, or CTAC, which combines the trade enforcement and intelligence capabilities of CBP and 12 other Federal agencies to protect the American public from unsafe imported products.

CTAC's joint targeting and enforcement efforts led to 243 seizures of unsafe products in 2017. Two months ago, CBP and CPSC targeting resulted in officers at the Port of Los Angeles seizing a large incoming shipment of toy building blocks for trademark infringement. These counterfeit toys were also found to violate the Federal Hazardous Substance Act for excessive lead and small parts.

We are concerned about the risks we find in rising volumes of small shipments, where 90 percent of our IPR seizures were made last year, and have been working with interagency and private-sector partners to address those risks.

Building on our experience in the CTAC and the clear mandate provided by Congress in TFTEA to develop an interagency approach to this critical type of enforcement, we have developed a draft joint import safety, rapid response plan. We will use this plan and follow-on interagency exercises to coordinate the management of incidents that present a safety risk to U.S. consumers and businesses.

In anticipation of future e-commerce growth and to manage threats in this environment, CBP is releasing a comprehensive e-commerce strategy which is critical for guiding our approach to enforcing intellectual property rights and enforcing import safety while supporting a vibrant and competitive sector of U.S. international trade.

We will work closely with all segments of the e-commerce community and our partner government agencies to identify information-sharing and other opportunities and pursue any necessary policy, regulatory, or statutory changes.

Chairman Hatch, Ranking Member Wyden, and distinguished members of the committee, I look forward to working with you to

build on these efforts, and thank you for the opportunity to testify today. I am happy to take any questions that you might have.

The CHAIRMAN. Well, thank you so much.

[The prepared statement of Ms. Smith appears in the appendix.]

The CHAIRMAN. Mr. Joholske, we will turn to you.

STATEMENT OF JIM JOHOLSKE, DIRECTOR, OFFICE OF IMPORT SURVEILLANCE, CONSUMER PRODUCT SAFETY COMMISSION, WASHINGTON, DC

Mr. JOHOLSKE. Thank you. Good morning, Chairman Hatch, Ranking Member Wyden, and distinguished members of the committee. Thank you for inviting me to discuss the U.S. Consumer Product Safety Commission's important role in protecting consumers from the health and safety hazards involving imports and counterfeit goods.

Before I begin, I should note that these comments are those of CPSC staff and they have not been reviewed or approved by and may not necessarily reflect the views of the Commission. I especially appreciate the opportunity to appear before you today, as this year marks the 10th anniversary of the creation of CPSC's Import Surveillance Program.

The CPSC was established by Congress in 1972 and is the Federal regulatory body charged with protecting the public from the unreasonable risk of injuries or death associated with consumer products. We are a relatively small agency with 545 full-time equivalents and a $125-million annual budget. However, we have jurisdiction over thousands of consumer products, a vast majority of which are imported into the United States.

Since the passage of the Consumer Product Safety Improvement Act of 2008, CPSC has strengthened its relationship with U.S. Customs and Border Protection and closely coordinates with CBP to interdict potentially noncompliant, unsafe imported products.

As part of our efforts, CPSC has placed investigators at the largest ports of entry to work side-by-side with CBP staff. Currently, we have 30 investigators stationed at 20 of the largest ports in the country. Despite our relatively small size, in fiscal year 2017 CPSC investigators at the ports screened more than 38,000 distinct products arriving in the United States and stopped approximately 4 million noncompliant or hazardous units from reaching consumers.

To prioritize and target high-risk shipments, CPSC has developed our own targeting system called RAM, or Risk Assessment Methodology. RAM leverages a feed of entry data received from CBP, which is combined with CPSC data to risk-score shipments under CPSC's jurisdiction.

We also have CPSC staff stationed at CBP's Commercial Targeting and Analysis Center to coordinate with CBP and other government agencies to address import safety hazards. CPSC also has a part-time presence at the National Intellectual Property Rights Coordination Center, where we exchange information with 22 partner agencies that may help us target potentially noncomplying and hazardous products.

As an agency with limited resources, we would not be able to do the critical work of intercepting high-risk products before they

reach consumers without the assistance and support of DHS and CBP.

Although CPSC's primary focus is targeting products that violate CPSC requirements, we do encounter intellectual property rights violations. Many of CPSC's investigators are former CBP officers and import specialists, and they have been trained to identify IPR issues. As a result, CPSC staff are often able to identify possible IPR violations in the course of their normal duties.

When CPSC identifies a potential IPR issue, we refer the shipment to CBP because they have the authority to efficiently seize the products. On a case-by-case basis, we will also test those IPR-violative products for compliance with CPSC mandatory standards or to determine whether they are otherwise hazardous.

CPSC and CBP have collaborated on many shipments where a potential IPR violation and a safety violation were found. Examples include holiday lights; cell phone wall chargers; lithium ion batteries used in hoverboards, laptops, and cell phones; children's backpacks; and numerous toys.

Although CPSC's import surveillance activities have prioritized large ports of entry, like many agencies we are facing challenges in regulating products imported through direct-to-consumer sales over e-commerce platforms. The volume of these shipments and the limited amount of data required when the shipment arrives in the United States make targeting difficult.

With CPSC's small size and limited resources, we currently do not have investigators stationed at locations where these small packages arrive, other than JFK Airport. However, CPSC will continue to evaluate its staffing model to identify efficient ways to target and examine potentially unsafe products shipped directly to e-commerce consumers.

Thank you for the opportunity to share my remarks. I am happy to answer any questions you may have.

The CHAIRMAN. Well, thank you so much.

[The prepared statement of Mr. Joholske appears in the appendix.]

The CHAIRMAN. Mr. Brady, we will conclude with you.

STATEMENT OF TERRENCE R. BRADY, PRESIDENT, UNDERWRITERS LABORATORIES, INC., NORTHBROOK, IL

Mr. BRADY. Good morning, Chairman Hatch, Ranking Member Wyden, distinguished members of the committee.

My name is Terrence Brady, and as the newly appointed president of Underwriters Laboratories, I am honored to appear before you today to share UL's experience combating the rise of counterfeit goods in e-commerce and to offer our perspectives on the challenges facing IP rights holders in this evolving global market.

UL is a global independent safety science company that has championed safety for nearly 125 years. Our 14,000 professionals around the globe are guided by our mission to promote safe living and working environments for people everywhere.

We use research, standards, and conformity assessment to meet ever-evolving safety challenges. We partner with manufacturers, retailers, trade associations, and regulatory authorities internation-

ally to provide solutions to address the risks of increasingly complex global supply chains.

UL takes counterfeiting very seriously, and we devote significant resources to fight it. We do this because we do not make or sell goods. Our product is our brand, our mark, which is built on a foundation of trust. When U.S. consumers see our UL mark, they know that an independent third party has determined that the manufacturer has demonstrated compliance with safety, performance, or other standards.

Unfortunately, the counterfeiters also recognize the value that UL brings, and they misappropriate our name and marks to try to legitimize the goods they sell.

Too often, consumers are unwitting victims of counterfeiting. They may suspect that the cheap handbag or watch they are buying is a knockoff, but many are entirely unaware that important other product categories are frequently counterfeited.

As the chairman noted, in 2016, we partnered with Apple to evaluate the dangers of counterfeit iPhone chargers like this small device. In a controlled test program, as the chairman stated, our engineers tested 400 counterfeit adapters bearing our UL marks, and the results were literally shocking. The overall failure rate exceeded 99 percent. And all but three adapters presented fire and shock risks. Twelve were so poorly made that they posed a direct risk of electrocution.

In 2017, we conducted over 1,200 investigations around the globe, resulting in the seizure of 1.5 million individual products. Let me give you a couple of highlights.

In terms of e-commerce, the focus of this hearing, we collected intelligence on more than 5,000 online listings across multiple platforms. We were able to identify more than 130 unique sellers with over 500 listings of counterfeit products.

We worked with the online platforms to remove the infringing listings and take appropriate actions against the sellers. As a result, law enforcement seized an estimated $660,000 worth of counterfeit smartphones, hard drives, flashlights, headlamps, and hoverboards.

Based on information UL provided, the DHS seized approximately 3,200 counterfeit UL safety labels and power adapters valued in excess of $200,000. And we partnered with the Los Angeles County Sheriff's Department to seize 2,500 counterfeit hoverboards and an additional 2,300 loose labels that the counterfeiters could stick on other fake goods.

These hoverboards, I should note, were shipped into the United States marked as wheelbarrows. The total seizure was valued at over $1.5 million.

Finally, UL cooperated with authorities on many other investigations, resulting in seizure of lithium ion batteries, fire sprinklers in buildings in India, household fans for use in Panama, and fake lifejackets for use in Peru, including those used for children.

My written testimony contains many more statistics and numbers than time permits here, but they underscore that the issue of counterfeiting extends to many product categories and countries.

In our 22-year history in this fight, we have deployed a comprehensive, multidimensional strategy based on three essential te-

nets: education, enforcement, and public/private partnerships. We work with our clients, with law enforcement, Customs officials, and others to stem the proliferation of counterfeits.

The issues we see in the traditional marketplaces are amplified in this borderless world of e-commerce. It was noted that online shipping and online direct-to-consumer sales have made it much harder for brands, law enforcement, and Customs officials to fight back, because the counterfeit penalties for a million dollars of counterfeit goods are far less than a million dollars' worth of drugs.

And as shippers go direct to consumers rather than risking an entire cargo container, this becomes very, very difficult. This is a challenge that legitimate platforms and IP rights holders have to work on together.

Thank you for the opportunity to testify today. UL welcomes the opportunity to work with you in the fight against counterfeits. And I welcome any questions the committee may have. Thank you.

The CHAIRMAN. Well, thanks to all four of you.

[The prepared statement of Mr. Brady appears in the appendix.]

The CHAIRMAN. Your testimony is really riveting. And it has to concern every American citizen, so we appreciate you taking the time to be here with us today, and we appreciate the work that you are doing and hope that you will step it up even more.

Ms. Gianopoulos, in your report you discuss two recommendations to CBP. Can you explain what factors make it difficult for CBP, ICE, and private-sector actors, such as websites and rights holders, to address the problem of counterfeits, and then reiterate why you feel the suggested changes will help address those concerns?

Ms. GIANOPOULOS. Thank you, Mr. Chairman. There are a number of things that are changing the e-commerce environment today. You could probably boil it down into three "v"s. There is the volume of goods, which each of us has talked about to some degree, where the number of shipments has just tremendously exploded over the past several years. So it is very difficult to focus in and find counterfeit goods on an individual-by-individual shipment basis.

There is also the value of those goods. The value has tremendously increased. I believe Ms. Smith talked a little bit about the seizure rate that has taken place, and that is just one factor that you can look at to determine how well seizures or how well enforcement is taking place.

And then finally, there is the variety. The variety of goods that are being counterfeited these days has just tremendously exploded. It is everything from YETI tumblers to duck decoys to kitchen sinks. So it is not something that a consumer or CBP or anyone for that matter can target as easily as they could in the past.

So our recommendations focus in on two of the things that the agencies can do to try to improve their processes.

First of all, in working with the private sector, while TFTEA did allow CBP to share more information, there are some restrictions on that sharing. And when we spoke with folks from the private sector, they expressed some concerns about their efforts to try to shut down these counterfeiters and the amount of information that

they needed in order to target their efforts as well. And they thought that that could be improved.

And then secondly, looking at the evaluation that could be done for CBP's and ICE's activities. Certainly, in a limited budget environment, as Federal agencies, we all want to put our money in the right places where it can do the most good. And we encouraged CBP to take additional steps to evaluate the activities it has underway in order to address some of these counterfeiting activities so that they can put their money in the best places.

The CHAIRMAN. Well, thank you.

Ms. Smith, as we have heard from GAO, CBP is really on the front lines of this quickly evolving problem or set of problems.

In your written testimony, you agreed with GAO's recommendations to better evaluate your IPR enforcement efforts and explore opportunities for better information sharing with the private sector. What steps do you plan to take to implement these recommendations?

Ms. SMITH. Senator, we think both of the recommendations were very productive ways for us to focus our efforts. The scope of the challenges, as the other witnesses have laid out, is tremendous. And one of the things that we have done to address GAO's recommendations is to charge our COAC E-Commerce Working Group to work with us to work through which information would be valuable to share and whom it should be shared with.

As you pointed out, TFTEA provides us good authority to share through properly promulgated regulations. And our intent is to address the issue of information sharing through additional regulatory framework.

The other thing that we have done to address some of the challenges that GAO identified is to develop and release today an e-commerce strategy to help us focus our efforts.

And we look forward to working with you and our colleagues here at the table to understand exactly where we can make the greatest impact.

The CHAIRMAN. Well, thank you so much.

Mr. Brady, UL has a vested interest in billions of individual products that are bought and sold each year. And as such, you have an important and valuable perspective, as I see it, in all of this. What steps do you as a company take to protect your intellectual property rights? And what can U.S. agencies do better to assist you in your efforts?

Mr. BRADY. Thank you, Mr. Chairman. As I noted earlier and as I think most of the people in the room know, our only product is trust. It is the trust that consumers place in us when they see our mark. And so we fight very hard to protect that trust because it is consistent with our 125-year-old mission of helping to create safe living and working environments for people everywhere.

Our team is small, but mighty; and therefore, we depend heavily on private/public partnerships to help us continue this fight against counterfeits.

What we need is real-time and transparent intelligence, because we rely on civil and criminal enforcement procedures beyond seizure and destruction. We pursue civil and criminal cases against the counterfeiters. If we bring stale data to the FBI or to the L.A.

County Sheriff, then they cannot do anything with it. So we need real-time intelligence sharing.

We are happy to and always share transparently with law enforcement and with government agencies what we find. We would like to reciprocate in that transparency and to keep the data fresh, because intelligence goes stale very quickly and these criminals quickly change their websites, their email addresses, their physical locations, their methods of shipment. They move fast. And we, together with government, need to move faster.

Thank you.

The CHAIRMAN. Well, thank you.

Senator Wyden?

Senator WYDEN. Thank you very much, Mr. Chairman.

I want to thank the panel.

And let me start with you, Ms. Smith. As I indicated, to me, what is going on is the rip-off artists, the counterfeiters, are trying to undercut the American brand. So this is really high-stakes stuff.

And I want to ask you the two questions that our staff asked your staff. And the first one is a "yes" or "no" answer so that we are clear on this. Does the agency need more authorities to crack down on the counterfeiters, the rip-off artists? That is just "yes" or "no," do you need more authority?

Because the staff asked it, and you all would not give a direct answer, so I want to give you the chance. "Yes" or "no," do you need more authority?

Ms. SMITH. Yes, Senator.

Senator WYDEN. Thank you. So that is good to finally have that on the record.

When will you be able to give us the details with respect to exactly what it is you need? Because as you know, the staff asked you, do you need more authority, and could not get an answer then. You have now given us an answer, to your credit.

And then they asked, can you tell us when we will get the details of what you need in this area and how you would like to proceed so we can up our game to be tougher on these counterfeiters? When will we get that?

Ms. SMITH. Senator, I think we should start the conversation now. But what I would recommend is that we gather the information about what data is available and whom it should come from and whom it should be provided to from our private-sector participants in the COAC E-Commerce Working Group.

I think it is important to have the private-sector perspective reflected. As you know, COAC is a very important intermediary provided for in TFTEA. And I would like to suggest that they work for several months so that we can come back to you as they are working and walk through what the recommendations are from the private sector.

Senator WYDEN. Now, you said we need time to have this conversation. We have been having this conversation for what feels like a longer-running battle than the Trojan War. It has gone on a long, long time. We know who the people are, the platforms, we know about the rights holders. I would like a date.

And I think you moved, again, in an encouraging way. Can we say within 60 days? As you said, you want to have this discussion

with the relevant private-sector parties; I am all for it. Can we have a commitment today that you will lay out for us what it is you are prepared to do in terms of this authority and that you will talk with the private parties within 60 days from today?

Ms. SMITH. Sir, I will do my best to meet that 60-day benchmark.

Senator WYDEN. Okay, good.

Let me turn now to the question of priorities and get your thoughts on this. I understand that the agency is moving to hire 5,000 Border Patrol agents here in the next 5 years and 2,000 officers. Now, I have supported billions of dollars in terms of security at the borders, and I am prepared to do what it is going to take to ensure that we protect the American people.

As you know, illegal crossings are now at a historic low. So how are we going to do it if we are putting twice as many people on this question of yet more agents at the border as we are in terms of getting the people we need to up our game in terms of the counterfeiters? How are we going to do it when that balance seems so out of whack?

Ms. SMITH. Senator, I think, as you have worked with us over many years to look at the very diverse portfolio of CBP's mission, to make sure that we have the right people on the border, whether they are wearing green uniforms, blue uniforms, or tan uniforms, you have also been very supportive of us in terms of making sure we have the expertise on the trade side.

As you know, the President's budget in fiscal year 2018 asked for 140 new positions to implement TFTEA. And I think that the combination of hiring those with trade expertise as well as those with border security responsibilities is a big challenge for CBP.

Senator WYDEN. You are being very diplomatic. And I am going to let you off the hook.

Ms. SMITH. Thank you, sir.

Senator WYDEN. I think you get my sense. I think the priorities are way out of whack when you have twice as many people in this area where the evidence shows that illegal activity is going down as opposed to what we are dealing with here.

And you are going to have a real—you described it as a challenge. I think the priorities are out of whack, and we need to get them straightened out.

One last question for—I believe this will be for Mr. Brady.

Mr. Brady, what I think you basically said—and I am going to direct the staff to look into it—you basically said that the rip-off artists, given the penalties, may, in effect, just say, hey, this is just the cost of doing business. Let us rip people off; the penalties are not that meaningful compared to the amount of business that we can rack up by doing all this counterfeiting and just moving online quickly and ripping people off.

That is pretty much what you are saying, right?

Mr. BRADY. That is exactly correct, Senator.

Senator WYDEN. Would you recommend to the chairman and me that, as part of this effort, we beef up the penalties, given what you have said, that they may, in effect, just be being treated as part of the cost of doing business?

Mr. BRADY. Yes, Senator. We would recommend that as a very fertile and important area to look into. We see evidence from, for

example the L.A. prosecutors, that counterfeiters get out very quickly and go right back to business the same day. They are actually trying civil suits against these people because they do not know how to manage a civil suit, but their jailhouse lawyers, they can get them out with a slap on the wrist today.

Senator WYDEN. I am way over my time. Could you furnish in writing to the chairman and me your thoughts of what might be a set of penalties that would ensure that this was not just, in effect, the cost of doing business? Could you furnish that to us?

Mr. BRADY. It will be our pleasure.

Senator WYDEN. Great.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Isakson?

Senator ISAKSON. Thank you, Mr. Chairman.

Ms. Gianopoulos, I was in the real estate business for a long time before I came to Congress and did a lot of retail shopping centers, and I have watched over the years the increase of sales over the Internet at Christmastime.

I think now, about 20 to 22 percent of sales at Christmas are made via the Internet and not by people going in the store and shopping and buying, which has exponentially grown retail sales over the Internet. Is it growing in a comparable way in other product lines, other times of the year?

Ms. GIANOPOULOS. You know, Senator, we did not take a look at the growth of e-commerce, per se. We were focused in on the challenges that were associated with e-commerce as it relates to counterfeits.

And as I said in my statement, it is very difficult when you are going online and just looking at a photo of an item to determine whether or not it is real. You may go into a store and be able to pick it up and see if it is a different weight or a different color or something like that.

But what some counterfeiters do is, they take the photo of the actual item and they put it online, even though they are giving you something that is counterfeit and it may not resemble that photo that you have seen online.

Senator ISAKSON. And then they produce a knockoff and sell it to you.

Ms. GIANOPOULOS. Absolutely.

Senator ISAKSON. Yes.

Ms. GIANOPOULOS. Or what they sometimes do is, they import the counterfeit items without the labels on them and then they import the labels separately and put the labels on in the United States.

Senator ISAKSON. Both ways are a problem for us, that is for sure.

Ms. GIANOPOULOS. Absolutely.

Senator ISAKSON. Ms. Smith, I have a habit of reading the resumes of people who come before us to just find out a little bit about them. I noticed you may be the person we really need to answer this question. I think Chairman Hatch asked it, and I think Senator Wyden did too.

But it says that you received the 2017 Distinguished Executive Presidential Rank Award. Is that correct?

Ms. SMITH. Yes, sir, it is.

Senator ISAKSON. And less than 1 percent of the executives in the Federal Government receive that award, and it is to recognize your achievement in enhancing CBP's enforcement to protect the American consumers.

Ms. SMITH. Yes, sir.

Senator ISAKSON. You ought to write the blueprint for this program then so you can cut through all the chaff that we have talked about and write that blueprint.

Ms. SMITH. We are working on it, sir.

Senator ISAKSON. In that particular situation, you did respond to the question asked by the ranking member about whether you need more authority. What authority specifically do you need more of to do your job?

Ms. SMITH. Sir, I believe that the authority request will touch on several things: the data that we can share and who we can share it with. I think, as Mr. Brady noted, that the penalties and the other civil enforcement actions that we can take in this area are also an important thing for us to consider and talk about.

The specifics—I would like to consult with both our other government agency partners and with the private sector to make sure that we are hitting the mark with it. But we will do that fairly quickly.

Senator ISAKSON. Is part of the problem the antitrust rules and regulations? Just out of curiosity.

Ms. SMITH. That has not been raised to us as an issue.

Senator ISAKSON. But it is a big enough problem, I think, in our country that we ought to weigh various barriers that we can for enforcement, not allow people to abuse it, but allow us to be able to enforce it.

Ms. SMITH. We will do that.

Senator ISAKSON. We appreciate all of you being here today and thank you for the good work that you do.

The CHAIRMAN. Well, thank you.

The Senator from Louisiana.

Senator CASSIDY. Ms. Smith, when a vendor is flagged as a possible seller of counterfeit goods, does that trigger an examination of their entire business, for example with other possible offenses like trade-based money laundering?

Ms. SMITH. Senator, it does. Once we have identified a particular business entity as a risk, we do try to take a broad-based approach to looking at all of their business activity.

We have some challenges, because oftentimes they will disappear and we need to find them through either corporate officers or other targeting information.

We are also looking to make sure that when we see a pattern of conduct from one business entity, that we look for that same pattern of conduct with similar types of businesses.

Senator CASSIDY. Now, that leads to my next question. Data analytics are being used by many in an attempt to winnow out and find that needle. And it sounds like you would start off with, is it

from China or is it from Hong Kong? But then you could pare it down, I presume. Is that being done?

Ms. SMITH. Yes, Senator, it is, but I think we can do more. There are some amazing developments in the technology space around predictive analytics.

CBP has used a number of tools over the years to target risk, but I think sort of the next frontier for us is around applying some of these innovative technologies to find that needle in a haystack.

Senator CASSIDY. Our office has been trying to figure out how well our agencies work together on trade-based money laundering. And I always point out, it is estimated cartels move $110 billion a year from the United States to Mexico, but we only confiscate, best as we can tell, about $7 billion.

Now, Senator Wyden spoke of the cost of doing business—we are only getting 5 percent of $110 billion. What would you say is the state of cooperation between the different agencies tasked with tracking trade-based money laundering and the other issues related to that and this panel?

Ms. SMITH. Senator, I think it is good. The cooperation——

Senator CASSIDY. Now, I have heard from others off the record that it is very bad, that it is siloed and that there is not the cooperation between agencies required for it to be effective. And I am not accusing, but if they are moving $110 billion a year and we are only getting $7 billion, it begs the question.

Ms. SMITH. I think this area, it is a very complex area. Trade-based money laundering is a fairly sophisticated version of trade violation.

I think it behooves us to take a whole-of-government approach, both from a criminal perspective and a civil perspective, and to apply the information that we can get from our intelligence agencies to both recognize and share that information to ensure that we are going after what is happening in real time.

Senator CASSIDY. I accept all of that conceptually. I guess what I am probing for is—if what I am hearing off the record is that it is not occurring now, how do we make that occur?

Ms. SMITH. I think by your message today, your question today to identify that as a high-risk area that the Congress is interested in. And then I think what we do is pull together those key agencies, whether it be ICE, whether it be the Department of Treasury, to focus on trade-based money laundering with a mandate to share information and take aggressive action.

Senator CASSIDY. Does anybody else on the panel have anything to offer on this particular topic?

Okay. I think I saw Mr. Brady nodding, so even though he is from UL, I thought maybe he had a thought on it.

Mr. BRADY. Senator, no, I have nothing to offer at this time.

Senator CASSIDY. Okay. Thank you, sir.

Let us see what else my interests lie in.

Using your current data analytics, are you able to identify both small shipments occurring through the mail, through the United States Postal Service, as well as larger shipments or shipments going through FedEx or DHL, UPS, et cetera?

Ms. SMITH. Yes, sir, we are. We get very good advanced electronic data in the express courier environment.

Senator CASSIDY. What about USPS?

Ms. SMITH. We are getting better. I think the advanced electronic data that we are seeing is not what we would like.

Senator CASSIDY. So when you say "better," that is a very elastic term. It could be from 1 percent to 2 percent, which would be a 100-percent improvement, but in absolute percentage it is pretty lousy.

So USPS, what percent of illicit or illegal or counterfeit goods do you feel that you are detecting when they come through USPS?

Ms. SMITH. We are getting advanced electronic data on approximately 50 percent of small packages in the postal environment now, which is significantly up. It represents data from 30 countries, which is significantly up from what we got 5 years ago, which was data from——

Senator Cassidy. Now, it sounds like Hong Kong and China are the ones that really matter.

Ms. SMITH. Yes.

Senator CASSIDY. So to what degree are you getting that from Hong Kong and China?

Ms. SMITH. We are getting all of the advanced electronic data from China. And Hong Kong, if you will give me just a moment—yes, Hong Kong as well. So we are getting that.

Senator CASSIDY. And so are we seizing illegal, illicit counterfeit goods from those areas?

Ms. SMITH. Yes, we are seizing counterfeit goods. We are also focused on things like fentanyl.

Senator CASSIDY. So what percent—this will be my last question. Thank you, Mr. Chairman.

What percent of the counterfeit illegal, illicit goods coming through the USPS do you feel you are confiscating—5 percent, 10 percent, 100 percent?

Ms. SMITH. Sir, I do not have an answer to that. And I think that is what GAO has asked us to look at. We will look at that going forward and try to get that estimate.

Senator CASSIDY. Okay, thank you. I yield back.

The CHAIRMAN. Okay.

The Senator from New Jersey.

Senator MENENDEZ. Thank you, Mr. Chairman, for holding today's hearing.

The United States is the world's leader in trusted and recognized brands, the ones most in demand, the ones that can command the best prices and, therefore, are the most vulnerable to knockoffs. That is why protecting our reputation and the investments we have put into it is so important.

Four years ago, families and businesses in New Jersey began contacting me about the increasing prevalence of counterfeit goods available for purchase online, particularly fake prom and wedding dresses. And it is a significant industry in New Jersey, but it is also significant to the people who end up at their wedding with something they totally did not expect.

This recent GAO report confirms what I have been hearing from so many of my constituents.

Now, the Trade Facilitation and Trade Enforcement Act that Congress passed in 2016 contained report language that I authored

with the chairman to raise the enforcement priority for fake products, specifically those shipped as gifts to avoid Customs duties and detection.

So, Ms. Smith, I know there has been a line of questioning on this, and I know that CBP has been working on this issue, but I am still unclear as to how the agency has implemented that language. Does a package marked as a gift that originates from a business address in a country like China, which is one of the worst offenders, which is documented by CBP and other sources as being a major source of counterfeits, trigger any red flags for our agents? Has the screening process changed since the passage of the Trade Enforcement and Facilitation Act?

Ms. SMITH. Senator, I think what we have done is to focus our targeting efforts in this area with specific targeting rules around gifts, as you note, which are identified as small packages, or other areas like household goods. That can be a generic description but may contain counterfeit goods, as we have seen in the past.

I think the other important area in this instance is to ensure that the representatives of the fashion industry and the folks whom your constituents are looking to buy safe, legitimate goods from, work with Customs and Border Protection to record their marks, to ensure that we know exactly what a legitimate product looks like and that we are working with that company to provide training to our officers and product information.

And we would be happy to work with you and your staff to do that.

Senator MENENDEZ. And my question is, do you have, are you using an algorithm? What are you using to actually flag something that is, quote unquote, "a gift" and is the preferred vehicle by which these counterfeit goods come to the United States?

Ms. SMITH. So we do have targeting algorithms, we call them rules, which knit together a variety of risk factors, both the description of the goods as gifts along with the high-risk countries that they may come from—China, Hong Kong—and then any additional information that we have about specific business entities—manufacturers, shippers, carriers—that previously may have brought counterfeit goods into the country will also be reflected in that targeting algorithm.

Senator MENENDEZ. Ms. Gianopoulos, did the GAO examine the CBP's efforts to screen these types of small, direct-to-consumer packages for counterfeit goods as opposed to larger shipments? And if you did, what did you find?

Ms. GIANOPOULOS. Well, in our work, while we did purchase 47 items and found 20 of them counterfeit, we did talk with CBP and ICE about their enforcement efforts.

We also put out a report last year where we looked at international mail facilities and looked at some of the differences between the information that CBP receives from those USPS facilities as opposed to express mail and found that the amount of information that CBP received from USPS was significantly less, because they are not required to put as much information that would be sent ahead of time to CBP. So CBP is limited in its ability to respond as opposed to, say, the express mail carriers where they are required to submit more information to CBP ahead of time.

Senator MENENDEZ. Is there a suggestion by the GAO on how to meet that challenge?

Ms. GIANOPOULOS. Well, one of the things we recommended in this report was for CBP and ICE to work more closely with the private sector to see what information would be most helpful for the private sector and CBP to share in order to address some of these counterfeit shipments, because some of the shipments are coming from within the United States. In fact, all 47 of the items that we purchased were shipped from U.S. addresses, so they would not have been able to use that Chinese or Hong Kong address as a flag because that is not where it was sent from to the consumer.

Senator MENENDEZ. One last question.

The CHAIRMAN. Senator, if I could interrupt. I am going to go vote, and so you will be the last questioner.

And I just want to thank everybody for being here. It has been a very informative hearing, and we will see what we can do to back you up and help you.

Ms. GIANOPOULOS. Thank you.

Senator MENENDEZ [presiding]. Thank you, Mr. Chairman.

One last question. On search engines, it seems to me that some online search engines and other websites aid and abet these counterfeiters by failing to police the use of copyrighted product imagery in online ads, that they may bear some responsibility.

It seems that the companies that sell online advertising have some capacity to prescreen advertisements and reject those that are found to be promoting an illegal or immoral product.

In fact, I have even heard that some search engines will remove counterfeit websites from their organic search results but continue to display those same companies' advertisements. In other words, some sellers of online ads may be continuing to receive advertising fees from companies they know to be breaking the law.

So if search engines like Google and social networks and other sellers of online ads are unwilling to filter these types of illegal advertisements, I hope and I look forward to working with the committee to explore policy options to address this threat to American businesses.

I wrote Google a letter last year asking them to address this issue and explain their policies on cracking down on advertisers of counterfeit goods, but I still have not had a response.

So the question for any of our witnesses is, in what ways should we look to cooperate with search engines and those who sell online advertising to make it more difficult for counterfeiters to reach their target audience? Are there ways to share additional information with these companies to make it easier to crack down on counterfeit ads? Does anybody have any insights into that?

Mr. BRADY. Senator, from UL's perspective and particularly given this shift to individual shipments from overseas directly to a U.S. home, we think the most important thing is to prevent that shipment and purchase in the first place.

Therefore, we think it is critical to work with the platforms and the search engines to shut down these people offering fake goods so the purchase never happens in the beginning. Once that little envelope leaves and heads to a constituent in your State, it is very, very hard for the authorities to intercept it.

So I think stopping the purchase in the first place by shutting down these bad websites is very important.

Senator MENENDEZ. Well, we look forward to it.

Ms. Smith, you have an idea?

Ms. SMITH. I just wanted to support what Mr. Brady said and also reiterate that we think that the platforms, the marketplaces, have to be part of the solution. They are sort of a new business entity for us that has popped up over the last couple of years. And I think we as a government community need to consider what their role, what their information is and what the expectations for them should be.

Senator MENENDEZ. Well, we look forward to following up on those.

Yes, Ms. Gianopoulos?

Ms. GIANOPOULOS. And I will address it from the other end of the spectrum as far as the consumers. If a consumer receives a product that is counterfeit, the websites that we spoke with were very anxious for those consumers to report it back to the website so they can take some action. If they do not know that the consumers are purchasing counterfeit items on their websites, it is difficult for them to do something about it.

So, as part of our recommendations in the appendix for consumers, suggestions we received from CPSC and others, we suggest that consumers report those counterfeit items promptly.

Senator MENENDEZ. Yes. And I appreciate doing that, and then they take it out of the organic search, which is a good thing, but they keep the advertisements on. So they are drawing revenue from the advertisements that they know are from counterfeit sites in the first place. So it seems to me if they take out the organic search, they should take out the advertisement as well.

So, on behalf of the chairman, we thank you all for being here and answering questions today.

Colleagues who have written questions are asked to submit them by the close of business next Friday, March the 16th.

And with that, this hearing is adjourned. Thank you very much.

[Whereupon, at 11:20 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF TERRENCE R. BRADY, PRESIDENT, UNDERWRITERS LABORATORIES, INC.

Good morning. Chairman Hatch, Ranking Member Wyden, distinguished members of the committee, my name is Terrence Brady. I am president of Underwriters Laboratories and formerly served as chief commercial and legal officer. I'm honored to appear before you today to share UL's experience combating the rise of counterfeit goods in e-commerce and to offer our perspective on the challenges facing intellectual property rights' holders in the evolving global market.

UL is a global, independent safety-science company that has championed safety for nearly 125 years. UL's 14,000 professionals are guided by our mission to promote safe working and living environments for people everywhere. We use research, standards, and conformity assessment to meet ever-evolving safety challenges. We partner with manufacturers, retailers, trade associations, and international regulatory authorities to provide solutions to address the risks of increasingly complex global supply chains.

UL takes counterfeiting very seriously and devotes significant resources to fight it. UL doesn't make or sell goods. Our product is our brand which is built on a foundation of trust. When consumers see the UL mark, they know that an independent third-party has determined that the manufacturer has demonstrated compliance with safety, performance, or other standards. Unfortunately, counterfeiters also recognize the value UL brings and they misappropriate our name and marks to try to "legitimize" the goods they sell.

Too often, consumers are unwitting victims of counterfeiting. They may suspect the inexpensive handbags or watches they're buying are knockoffs, but many are unaware that other product categories are frequently counterfeited. UL has investigated instances of counterfeit smoke alarms, fire extinguishers, sprinklers, circuit breakers, extension cords, life preservers, and—as the Government Accountability Office (GAO) report demonstrates—phone chargers.

In 2016, UL partnered with Apple to evaluate the dangers of counterfeit iPhone chargers. In a controlled test program, our engineers tested 400 counterfeit adapters bearing UL marks and the results were literally shocking: the overall failure rate exceeded 99 percent. All but three adapters presented fire and shock hazards. Twelve were so poorly made that they posed a risk of electrocution.

In 2017, our Global Security and Brand Protection team conducted over 1,200 investigations of suspected counterfeit UL marked products resulting in the seizure of 1.5 million units. The top four cases by product type included power supplies, batteries, surface-mounted lights and cord sets. Let me offer a few highlights.

- Approaching the holiday season, we began a global 2-month investigation of counterfeit operations in southern California involving UL marks. We surveyed 290 locations across the United States and Mexico, observing products from approximately 14,000 separate entities including brick and mortar stores and flea markets. We made over 230 test purchases, uncovering 150 vendors distributing products with illicit UL marks. In addition, we collected intelligence on more than 5,000 online listings across multiple platforms. We were able to identify more than 130 unique sellers with over 500 listings of counterfeit products. UL worked with the online platforms to remove the infringing listings and take appropriate actions against the sellers. We deter-

mined that 27 sellers needed further investigation, and we made a series of test purchases. These purchases led to the successful raid of two warehouses in California where officials seized an estimated $660,000 of potentially dangerous products bearing counterfeit UL marks. The products seized included counterfeit iPhones and iPhone batteries, Microsoft360 hard drives, Cree flash lights and headlamps, clapper devices, and hoverboards.

- In February, UL helped the Department of Homeland Security execute a search warrant in a case arising from a 2-year investigation of an online distributor of power adapters. Based on the information UL provided, DHS seized approximately 3,227 counterfeit UL labels and adapters valued in excess of $200,000.
- Last September, UL partnered with the Los Angeles County Sheriff's Department Counterfeit and Piracy Enforcement team to execute a search warrant at a warehouse in Santa Fe Springs, CA. During the search warrant, a total of 2,510 hoverboards bearing counterfeit holographic UL labels were seized. These hoverboards were shipped into the United States as "wheelbarrows" according to the shipping label. While assisting the Sheriff's team with the search and inspection of the location, UL also recovered 2,325 counterfeit holographic UL labels. The total seizure amount for the hoverboards and labels is estimated at $1.5 million dollars.
- Finally, UL cooperated with law enforcement and Customs authorities on other investigations, resulting in the seizure of:
  - 77,972 lithium ion batteries bearing a counterfeit UL mark—10,000 of which also bore a counterfeit Apple trademark;
  - 5,143 counterfeit sprinklers in India;
  - 42,000 counterfeit household fans in Panama; and
  - 200 counterfeit life jackets in Peru—particularly troubling given that suspect company made and sold children's life jackets.

These few examples illustrate the pervasiveness of the problem and underscore that counterfeiting is not limited to any one category of products or a problem in the United States alone. Counterfeit goods directly threaten human lives.

In our 22 years of experience combating counterfeiting, UL has deployed a comprehensive, multi-dimensional strategy based on three essential tenets: education, enforcement, and partnerships. We work with our clients, law enforcement officers, Customs officials, and others to stem the proliferation of counterfeits. I have already illustrated some of our investigations and collaboration with government. Additionally, under our strategy we have:

- Partnered with INTERPOL to establish the International Intellectual Property Crime Investigators College to educate law enforcement officials and Customs agents to recognize and identify legitimate safety certification marks;
- Processed approximately 25,000 product authentication requests to identify counterfeit UL Marked products as part of our Border Protection Program; and
- Worked extensively with the International Anti-Counterfeiting Coalition and Michigan State University's A–CAPP Center to support research on counterfeiting and to develop programs to reduce its impact.

The counterfeiting issues we see in traditional marketplaces are amplified in the borderless world of e-commerce. The growth in recent years of counterfeit products has been facilitated in part by shifting consumer preferences for shopping online and the proliferation of online merchants. And in recent years, this scourge has become much harder for brands, law enforcement, and Customs to fight as the counterfeiters realized the criminal penalties for $1 million worth of counterfeit consumer goods are far less severe than an equivalent amount of drugs, and as they increasingly shift to air-shipping orders directly to consumers rather than smuggling an entire cargo container.

Selling counterfeits online with individual shipments makes it easier to fly under the radar of law enforcement and IP rights' holders. Most major online retailers have clear anti-counterfeiting policies and actively respond to reports of counterfeit products marketed through their retail platforms; that said, the sheer volume of goods offered for direct-to-consumer purchase make it extremely difficult to discover counterfeiters who regularly change identities to avoid detection. Some lesser-known sellers and platforms openly market fake products. This is a challenge that legiti-

mate e-commerce platforms and IP rights' holders must navigate together, working with all law enforcement including Customs authorities, regulators, lawmakers, and other parties.

UL's commitment to fight counterfeiting is unwavering and we welcome opportunities to work with like-minded stakeholders to address known and emerging problems. UL commends this committee for your leadership on this issue and for recognizing that more must be done to combat the proliferation of counterfeit goods. UL recommends:

- **Continued collaboration between the public and private sectors:** As UL's experience illustrates, this complex problem requires IP rights' holders, e-commerce platforms, brick and mortar retailers, government, and others to work together to fight counterfeits and educate consumers about the dangers they pose. Robust information-sharing amongst all parties is critical to bring counterfeiters to justice and fully maximize the potential of public-private partnerships to address IP violations.
- **Strong IP protections and enforcement mechanisms in trade agreements:** Strong and effective protection and enforcement of intellectual property rights is critical to U.S. economic growth and American jobs. Trade agreements—whether bilateral or multilateral—should build on the foundations established in existing international IP agreements and establish strong protections for patents, trademarks, copyrights, and trade secrets. In any trade agreement, it is important to secure strong and fair enforcement rules to protect against trademark counterfeiting and copyright piracy, including rules allowing increased penalties in cases where counterfeit or pirated goods threaten consumer safety or health. Congress should encourage the administration to include such provisions in any trade agreements it negotiates.
- **Tougher penalties and dedicated resources for enforcement and education:** The United States has enacted some of the strongest intellectual property protections in the world, a critical need for rights' holders. To ensure their enforcement, Congress and the administration should prioritize funding for agencies such as U.S. Customs and Border Protection to combat counterfeiting and close loopholes that allow counterfeits to flow across borders. In addition, Congress should ensure that the U.S. Consumer Product Safety Commission continues to have the resources it needs to conduct its work and to educate manufacturers, importers, consumers, and others about product safety issues, including the dangers posed by counterfeit goods.

Chairman Hatch, Ranking Member Wyden, members of the committee, thank you for the opportunity to testify today. UL welcomes the opportunity to work with you in the fight against counterfeits. I welcome any questions you may have.

PREPARED STATEMENT OF KIMBERLY GIANOPOULOS, DIRECTOR, INTERNATIONAL AFFAIRS AND TRADE, GOVERNMENT ACCOUNTABILITY OFFICE

Chairman Hatch, Ranking Member Wyden, and members of the committee, I am pleased to be here to discuss the results of our review of U.S. agencies' efforts to address changes in the market for counterfeit goods and their work with the private sector. Intellectual property is an important component of the U.S. economy, and the United States is an acknowledged global leader in its creation. Infringement of intellectual property rights (IPR) through the illegal importation and distribution of counterfeit goods harms the U.S. economy by stifling innovation, slowing economic growth, weakening the competitiveness of U.S. employers, and threatening American jobs.[1] IPR infringement can also threaten the health and safety of American consumers. The Department of Homeland Security's U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE)—two of the many agencies involved in IPR enforcement—are responsible for IPR enforcement at U.S. borders. CBP leads enforcement activity at the border by detecting and seizing counterfeit goods that enter the United States through its more than 300 ports of entry and by assessing penalties against IPR infringers. CBP coordinates its efforts with ICE, which investigates IPR violations for Federal prosecution.

[1] In this statement, "counterfeit goods" refers to any physical goods that are found to be in violation of trademark or copyright law.

My testimony today summarizes the findings from our January 2018 report,[2] which was released on February 27, 2018, on CBP's and ICE's IPR enforcement at U.S. borders. This testimony addresses (1) what is known about counterfeit goods entering the United States and the challenges they present, (2) efforts CBP and ICE have undertaken to enhance IPR enforcement and the extent to which they have assessed the results of these efforts, and (3) the extent to which CBP and ICE collaborate on IPR enforcement as well as ways in which they coordinate with the private sector in enforcing IPR.

For our report, we analyzed CBP seizure data for fiscal years 2012 through 2016 and reviewed documents and reports from CBP, ICE, other U.S. Government entities, and international organizations. We interviewed CBP and ICE officials in Washington, DC, and at selected port locations in Chicago, IL; Los Angeles, CA; Miami, FL; and New York, NY. We also interviewed representatives of IPR-holding companies (rights holders) and popular consumer websites that offer platforms for third-party sellers. We used undercover identities to purchase selected products from third-party sellers on popular consumer websites and subsequently asked the rights holders for the selected products to test their authenticity. More detailed information on our objectives, scope, and methodology for this work can be found in the issued report. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work in accordance with investigation standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

ACCELERATED BY E-COMMERCE, CHANGES IN THE COUNTERFEITS MARKET PRESENT CHALLENGES TO U.S. AGENCIES, CONSUMERS, AND THE PRIVATE SECTOR

E-Commerce Has Contributed to a Shift in the Market for Counterfeit Goods

The rise of e-commerce has contributed to a fundamental change in the market for counterfeit goods, according to our analysis of documents from CBP, ICE, and international organizations and our interviews with CBP and ICE officials. U.S. agencies and international organizations have observed a shift in the sale of counterfeit goods from "underground" or secondary markets, such as flea markets or sidewalk vendors, to primary markets, including e-commerce websites, corporate and government supply chains, and traditional retail stores. Whereas secondary markets are often characterized by consumers who are knowingly purchasing counterfeits, primary markets involve counterfeiters who try to deceive consumers into purchasing goods they believe are authentic.

This shift has been accompanied by changes in the ways in which counterfeit goods are sold. In the past, consumers could often rely on indicators such as the location of sale or the goods' appearance or price to identify counterfeit goods in the marketplace. However, counterfeiters have now adopted new ways to deceive consumers. For example, as consumers increasingly purchase goods online, counterfeiters may exploit third-party online marketplaces to gain an appearance of legitimacy and access to consumers. When selling online, counterfeiters may post pictures of authentic goods on the websites where they are selling counterfeits and may post pseudonymous reviews of their products or businesses in order to appear legitimate. Additionally, by setting the price of a counterfeit at, or close to, the retail price of a genuine good, counterfeiters may deceive consumers, who will pay the higher price because they believe the goods are real or who believe that they are getting a slight bargain on genuine goods.

CBP Data Indicate Changes in Several Key Characteristics of Counterfeit Goods Seized

According to CBP seizure data and CBP officials, the volume, variety, and methods of shipment of counterfeit goods seized by CBP and ICE have changed in recent years. CBP reports indicate that the number of IPR seizures increased by 38 percent in fiscal years 2012 through 2016. According to CBP data, approximately 88 percent of IPR seizures made during this period were shipped from China and Hong Kong. The variety of products being counterfeited has also increased, according to CBP officials. CBP and ICE officials noted that, while many consumers may think of lux-

[2] GAO, "Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market," GAO–18–216 (Washington, DC: January 30, 2018).

ury handbags or watches as the most commonly counterfeited goods, counterfeiting occurs in nearly every industry and across a broad range of products. In addition, according to CBP data we reviewed and officials we spoke to, the methods of importing counterfeit goods into the United States have changed in recent years. Specifically, express carriers and international mail have become the predominant form of transportation for IPR-infringing goods entering the United States, constituting approximately 90 percent of all IPR seizures in fiscal years 2015 and 2016, according to CBP data.

Twenty of 47 Items Purchased From Third-Party Sellers on Popular E-Commerce Websites Were Counterfeits, Highlighting Potential Risks to Consumers

In an attempt to illustrate the risk that consumers may unknowingly encounter counterfeit products online, we purchased a nongeneralizable sample of four types of consumer products—shoes, travel mugs, cosmetics, and phone chargers—from third-party sellers on five popular e-commerce websites.[3] According to CBP data we reviewed and officials we spoke to, CBP often seizes IPR-infringing counterfeits of these types of products. As table 1 shows, the rights holders for the four selected products we purchased determined that 20 of the 47 items were counterfeit.

Table 1: Results From Rights-Holder Testing of GAO Covert Purchases of Four Frequently Counterfeited Consumer Products

	Nike Air Jordan shoes	Yeti travel mugs	Urban Decay cosmetics	UL-certified phone chargers	Total
Authentic	15	3	0	9	27
Counterfeit	0	6	13	1	20
Total	**15**	**9**	**13**	**10**	**47**

Source: GAO–18–383T.

Note: We asked the rights holders for the four products to test a total of 47 items that we purchased from third-party sellers on five popular e-commerce websites. These results do not include one charger that we excluded from testing. Despite being advertised as UL-certified, the product arrived without a certification seal and therefore could not be tested for authenticity.

We did not identify any clear reasons for the variation among the counterfeit and authentic items that we purchased based on the products that they represented, the e-commerce websites where we bought the items, or the third-party sellers from whom we bought them. For three of the four product types, at least one item we purchased was determined to be counterfeit, with results varying considerably by product. Representatives of the rights holders also could not provide a specific explanation for the variation among authentic and counterfeit goods that we received. They noted that the results of covert test purchases can fluctuate depending on enforcement activities and the variety of goods and sellers on a particular website on a given day. Rights-holder testing also showed that we purchased at least one counterfeit item and one authentic item from each of the five e-commerce websites. In addition, our analysis of the customer ratings of third-party sellers from whom we bought the items did not provide any clear indications that could warn consumers that a product marketed online may be counterfeit. For example, we received both counterfeit and authentic items from third-party sellers with ratings that were less than 70 percent positive as well as sellers with ratings that were up to 100 percent positive.

Rights holders were able to determine that items we purchased were not authentic on the basis of inferior quality, incorrect markings or construction, and incorrect labeling. Some counterfeit items we purchased were easily identifiable as likely counterfeit once we received them. For example, one item contained misspellings of "Austin, TX" and "Made in China." Other items could be more difficult for a typical consumer to identify as counterfeit. For example, the rights holder for a cosmetic product we purchased identified one counterfeit item on the basis of discrepancies

[3] All 47 items we purchased were shipped from U.S. addresses, signifying that any items manufactured outside the United States were imported before being sent to us. Rights holders confirmed that at least a portion of the authentic versions of the products purchased are manufactured abroad. Additionally, according to a 2011 IPR Center report, most physical counterfeit goods are manufactured abroad. Final production of some counterfeit items, such as applying labels and packaging items, may take place after items are imported into the United States.

in the color, composition, and design of the authentic and counterfeit items' packaging. Counterfeit goods may also lack key elements of certification markings and other identifiers. For example, on a counterfeit phone charger we purchased, the UL certification mark did not include all components of the authentic mark. Figure 1 shows examples of these counterfeit items.

Figure 1: Examples of Some Counterfeit Items Purchased Online

Source: GAO, Urban Decay (cosmetic photos). | GAO-18-383T

The risks associated with the types of counterfeit goods we purchased can extend beyond the infringement of a company's IPR. For example, a UL investigation of counterfeit iPhone adapters found a 99 percent failure rate in 400 counterfeit adapters tested for safety, fire, and shock hazards and found that 12 of the adapters tested posed a risk of lethal electrocution to the user.[4] Similarly, according to a rights holder representative, counterfeits of common consumer goods, such as Yeti travel mugs, may contain higher-than-approved concentrations of dangerous chemicals such as lead, posing health risks to consumers. According to ICE, seized counterfeit cosmetics have been found to contain hazardous substances, including cyanide, arsenic, mercury, lead, urine, and rat droppings.

Representatives of rights holders and e-commerce websites whom we interviewed reported taking independent action to try to protect IPR within their areas of responsibility. For example, both rights holders and e-commerce websites maintain IPR protection teams that work with one another and with law enforcement to address infringement issues. E-commerce websites may also take a variety of steps to block and remove counterfeit items listed by third-party sellers. These efforts rely on data collected through a variety of means, including consumer reporting of counterfeits, rights-holder notifications of IPR infringement, and corporate efforts to vet potential third-party sellers, according to private sector representatives.

Our January 2018 report includes information on steps that consumer protection organizations and government agencies recommend consumers take to limit the risk of purchasing counterfeits online. These steps include, for example, buying only from authorized retailers online, avoiding prices that look "too good to be true," and reporting counterfeit purchases.

Changes in the Marketplace Can Pose Challenges to U.S. Agencies and the Private Sector

We identified a number of key challenges that the changes in the market for counterfeit goods can pose to CBP and ICE as well as to the private sector. First, the increasing sophistication of counterfeits can make it difficult for law enforcement officers to distinguish between legitimate and counterfeit goods. Second, as the range of counterfeit goods expands, CBP has a wider variety of goods to screen, which requires CBP officials to have in-depth knowledge of a broad range of products and

[4] UL, "Counterfeit iPhone Adapters: A UL Technical Investigation Shows a 99 Percent Failure Rate" (2016).

of how to identify counterfeits. Third, counterfeiters may break up large shipments into multiple smaller express carrier or mail packages to decrease the risk of losing significant quantities of merchandise to a single seizure. This shift toward smaller express shipments of counterfeit goods to the United States poses challenges to CBP and ICE because, according to CBP officials, seizure processing requires roughly the same amount of time and resources regardless of shipment size or value.

The changing marketplace also presents challenges to the private sector, according to representatives from rights holders and e-commerce websites. For example, it is more difficult for rights holders and e-commerce websites to identify and investigate individual counterfeit cases, because e-commerce websites face a growing inventory from a larger registry of sellers. Tracking goods from known counterfeiters through various website fulfillment and delivery mechanisms is also a significant challenge for the private sector. Furthermore, the growth of e-commerce has accelerated the pace at which counterfeiters can gain access to consumers or reinvent themselves if shut down.

CBP AND ICE ENGAGE IN ACTIVITIES TO ENHANCE IPR ENFORCEMENT, BUT CBP HAS NOT FULLY EVALUATED THE RESULTS OF ITS ACTIVITIES

CBP and ICE engage in a number of activities to enhance IPR enforcement; however, while ICE has assessed some of its efforts, CBP has taken limited steps to do so. CBP's and ICE's IPR enforcement activities broadly include detecting imports of potentially IPR-infringing goods, conducting special operations at U.S. ports, engaging with international partners, and undertaking localized pilot programs or portled initiatives. CBP and ICE have collected some performance data on activities we reviewed, and ICE has taken some steps to better understand the impact of its efforts, such as creating a process to track cases it deems significant. However, we found that CBP has conducted limited evaluation of its efforts to enhance IPR enforcement. Consequently, we concluded that CBP may lack information needed to ensure it is investing its resources in the most efficient and effective activities. We recommended in our report that CBP take steps to evaluate the effectiveness of its IPR enforcement efforts; CBP concurred with this recommendation.

CBP AND ICE GENERALLY COLLABORATE ON IPR ENFORCEMENT, BUT CBP IS RESTRICTED IN SHARING INFORMATION WITH THE PRIVATE SECTOR

Our analysis showed that CBP and ICE interagency collaboration on IPR enforcement is generally consistent with the following selected key practices for effective interagency collaboration: (1) define and articulate a common outcome; (2) establish mutually reinforcing or joint strategies; (3) identify and address needs by leveraging resources; (4) agree on roles and responsibilities; and (5) establish compatible policies, procedures, and other means to operate across agency boundaries.[5] For example, the agencies may leverage resources by collocating staff or sharing their expertise. CBP and ICE have also issued guidance and developed standard operating procedures to clarify roles and responsibilities. CBP and ICE also coordinate with the private sector in a variety of ways, such as obtaining private sector assistance to determine whether detained goods are authentic and to conduct training.

Representatives of rights holders and e-commerce websites noted that information shared by law enforcement entities is critical to private-sector IPR enforcement, such as pursuing civil action against a counterfeiter or removing counterfeit items from websites. In the Trade Facilitation and Trade Enforcement Act of 2015, Congress provided CBP with explicit authority to share certain information with trademark and copyright owners before completing a seizure.[6] CBP officials stated that they share information about identified counterfeits with e-commerce websites and rights holders to the extent possible under current regulations. However, according to private sector representatives we spoke to, restrictions on the amount and type of information about seized items shared by CBP limit the ability of rights holders and e-commerce websites to protect IPR. CBP officials noted that there are legal

[5] GAO, "Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration Among Federal Agencies," GAO–06–15 (Washington, DC: October 21, 2005). Our October 2015 report listed eight practices that can enhance and sustain interagency collaboration. Our January 2018 report evaluated CBP's and ICE's collaboration on IPR enforcement against five of these practices, which we selected because we determined they were most relevant to that review.

[6] This authority applies only with respect to goods suspected of infringing a trademark or copyright that is recorded with CBP. Pub. L. No. 114–125, § 302(a), 130 Stat. 122, 149 (2016).

limitations to the amount and type of information they can share, particularly if the e-commerce website is not listed as the importer on forms submitted to CBP.

Several private sector representatives stated that receiving additional information from CBP would enhance their ability to protect IPR. Representatives of one website noted that information on the exterior of seized packages, such as business identifiers on packages destined for distribution centers, would be helpful for identifying groups of counterfeit merchandise from the same seller. However, according to CBP officials, CBP cannot provide such information to e-commerce websites. Representatives of one e-commerce website noted that ICE sometimes shares information related to an investigation, but that ICE's involvement in the enforcement process begins only after CBP has identified and seized counterfeit items. Representatives of two e-commerce websites stated that, because of the limited information shared by CBP, they may not be aware of IPR-infringing goods offered for sale on their websites, even if CBP has seized related items from the same seller.

According to CBP officials, CBP is reviewing options for sharing additional information with rights holders and e-commerce websites and is assessing what, if any, additional information would be beneficial to share with private-sector entities. CBP officials stated that they have not yet determined whether changes to the amount and types of information provided to e-commerce websites would require regulatory changes or additional legal authorities. These officials also said that they have discussed differences in CBP's and ICE's information sharing with ICE officials. In our report, we recommended that CBP, in consultation with ICE, assess what, if any, additional information would be beneficial to share with the private sector and, as appropriate, take action to enhance information sharing where possible. CBP concurred with this recommendation.

Chairman Hatch, Ranking Member Wyden, and members of the committee, this concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.

QUESTIONS SUBMITTED FOR THE RECORD TO KIMBERLY GIANOPOULOS

QUESTIONS SUBMITTED BY HON. ORRIN G. HATCH

Question. Why should consumers be concerned about the findings in your report related to the prevalence of counterfeit products? And how can consumers best protect themselves from the risks of purchasing counterfeit goods online?

Answer. Counterfeit goods may pose numerous risks to the health and safety of consumers. For example, counterfeit personal care products may pose risks including damage to skin or eyes caused by dangerous chemicals and bacteria. Additionally, counterfeit electronic devices can pose a safety hazard. For example, counterfeit hair removal devices, hair curlers and straighteners, and skin cleansing devices run the risk of burning or electrocution due to nonstandardized wiring. U.S. Immigration and Customs Enforcement (ICE) has also investigated intellectual property (IP) crimes involving counterfeit airbags, steering, braking, and seatbelt components, bearings, and diagnostic equipment.

The sale of counterfeit goods can also pose a threat to national security and to the U.S. economy. For example, U.S. Customs and Border Protection (CBP) and ICE have seized and investigated counterfeit goods, such as integrated circuits, destined for Department of Defense supply chains. Additionally, counterfeiting has been linked to transnational organized crime and terrorist organizations. According to the United Nations Office of Drugs and Crime, the illicit trafficking of counterfeit goods is an increasingly attractive avenue for criminal organizations to diversify their product range. In 2010, we reported that counterfeiting also posed a wide range of economic risks to consumers, industry, government, and the economy as a whole. Counterfeiting's economic effects on consumers include, for example, financial losses resulting from counterfeit products that fail due to inferior quality. In addition, counterfeiting may pose risks to industry and government by increasing intellectual property rights (IPR) protection and enforcement costs, by affecting sales and brand value for the businesses whose products are counterfeited, and by potentially reducing tax revenue collected by the government.

Our January 2018 report includes an appendix outlining tips from consumer protection organizations and government agencies on ways in which consumers can

limit the risk of purchasing counterfeits online.[1] This appendix includes recommendations such as reviewing the seller listed on the product page to determine whether it is a third party. For example, if an item's listing says it is "fulfilled by" a website, that does not necessarily mean it is "sold by" that website. Additionally, consumers can look for external trust-building features associated with third-party sellers, such as a mail address or telephone number, real-time customer service, or verifiable external accreditation. According to rights holders we interviewed, the safest option is to buy directly from them or their authorized retailers.

Question. When you were making your purchases, did you find any details such as consumer reviews or prices that indicated whether a product was counterfeit or authentic?

Answer. For the items we purchased, we did not find customer reviews to be a reliable indicator of product legitimacy. Specifically, our analysis of the customer ratings of third-party sellers from whom we made purchases did not provide any clear indications that could warn consumers that a product marketed online may be counterfeit. For example, we received both counterfeit and authentic items from third-party sellers with ratings that were less than 70 percent positive as well as sellers with ratings that were up to 100 percent positive. Counterfeiters may take steps to artificially inflate their reviews, such as by posting pseudonymous reviews of their products or businesses.

We did not find a clear link between price and the authenticity of the products we purchased. For example, for two of the four product types we purchased, the highest-priced item we ordered was counterfeit, while for the other two product types, the highest-priced item we ordered was authentic. Similarly, for two of the four product types we purchased, the lowest- priced item we ordered was counterfeit, while for the other two product types, the lowest-priced item we ordered was authentic. U.S. agencies have reported that counterfeiters may set prices close to the retail price of a genuine good as a method of deceiving consumers into believing the goods are real. However, consumer protection organizations note that pricing significantly lower than MSRP can still be an indicator that a good may not be genuine.

Question. What factors make it difficult for CBP, ICE, and private-sector actors, such as websites, to address the problem of counterfeits?

Answer. We identified a number of key challenges that the changes in the market for counterfeit goods can pose to CBP and ICE as well as to the private sector. First, the increasing sophistication of counterfeits can make it difficult for law enforcement officers to distinguish between legitimate and counterfeit goods. Second, the increased variety and volume of counterfeit goods crossing the border complicate enforcement efforts because CBP officers must screen a wider variety of goods and have in-depth knowledge of a broad range of products. Third, shifts in the mode of transportation of counterfeit goods to the United States pose additional challenges to CBP and ICE. For example, seizures have become less of a deterrent for counterfeiters who break up large shipments into multiple smaller express carrier or mail packages. Each of these smaller packages includes fewer goods than a single large shipment, decreasing the counterfeiter's risk of losing significant quantities of merchandise to a single seizure. Fourth, counterfeiters may attempt to deceive law enforcement or evade detection, such as by separating IPR-infringing labels from counterfeit goods during the transportation process and then completing the labeling and packaging of the goods in the United States. Finally, CBP and ICE officials noted that targeting the root causes of IPR infringement requires international cooperation to disrupt the networks that produce, sell, and ship counterfeit goods and some countries are more receptive to working with U.S. agencies than others.

Private-sector entities, such as rights holders and e-commerce websites, also face challenges in protecting IPR, including managing a large inventory and growing registry of sellers on individual e-commerce websites and overall growth in the number of such websites. This makes it difficult for both websites and rights holders to identify and investigate individual counterfeit cases, as well as track possible counterfeit goods and sellers. Representatives from rights holders and e-commerce websites noted that limited information sharing from CBP following a seizure complicates their efforts to protect IPR. We recommended that CBP, in consultation with ICE, assess what, if any, additional information would be beneficial to share with the pri-

[1] GAO, "Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market," GAO–18–216 (Washington, DC: January 30, 2018).

vate sector and, as appropriate, take action to enhance information sharing such as by proposing regulatory changes or requesting additional legal authorities.

QUESTION SUBMITTED BY HON. RON WYDEN

Question. In one way or another, you all touched on the shift from containerized shipping to small packages. You have also highlighted the challenges in enforcement against counterfeit goods.

Given that we seem to be in a new era of trade, wouldn't you agree that the Federal Government's enforcement strategy to go after counterfeit goods needs to adapt to the changing market? If so, what changes would you recommend in current CBP and ICE enforcement priorities and approaches?

Answer. We did not review the government's overall strategy to countering IPR infringement. However, we noted in our report that changes in the marketplace, including the shift toward smaller packages, have presented challenges to CBP. While CBP has undertaken some efforts to enhance enforcement given the changing environment, such as by developing a targeting model for express carrier shipments and piloting alternative approaches to seizures for small packages, we found that it has not evaluated the effectiveness of its efforts. We recommended that CBP take steps to evaluate the effectiveness of its IPR enforcement efforts in order to focus its resources on the most efficient or effective efforts.

Given the changes in the marketplace, including the fact that counterfeiters may try to use popular e-commerce websites to gain an appearance of legitimacy and reach consumers, it is important for CBP to ensure it is coordinating effectively with the private sector. Private-sector representatives told us that receiving additional information from CBP, such as business identifiers on the exterior of seized packages destined for distribution centers, could enhance their ability to protect IPR. Accordingly, we recommended that CBP, in consultation with ICE, assess what, if any, additional information would be beneficial to share with the private sector and, as appropriate, take action to enhance information sharing such as by proposing regulatory changes or requesting additional legal authorities.

QUESTION SUBMITTED BY HON. JOHN THUNE

BEST PRACTICES OF FOREIGN CUSTOMS AGENCIES;
CBP INTERACTION WITH FOREIGN CUSTOMS AGENCIES

Question. The GAO report notes that some European customs agencies are able to share more information than CBP.

Ms. Gianopoulos, during your investigation, did you look at any best practices used by other foreign customs agencies? If so, can you comment on any best practices that CBP should take into account or that should be implemented but would require statutory authority?

Answer. We did not explore or evaluate best practices used by other foreign customs agencies. Representatives of one of the rights holders we interviewed noted that European customs agencies provide more information following a seizure than CBP, which enhances the rights holder's ability to take action following a seizure. While we did not evaluate differences in statutory authority between the United States and other countries, we did recommend that CBP assess what additional information it can share with the private sector and, as appropriate, take action to enhance information sharing, where possible, such as by proposing regulatory revisions or requesting additional legal authorities.

QUESTIONS SUBMITTED BY HON. MARIA CANTWELL

Question. As the GAO report identifies, CBP does not proactively communicate with online marketplaces that have teams that work closely with the intellectual property rights center, brands, and law enforcement to keep counterfeit items off their sites. However, information sharing is critical.

What are the specific legal parameters for sharing information with e-commerce websites about counterfeit goods CBP seizes?

Answer. According to CBP officials, with regard to an IPR seizure, CBP is legally allowed to share (1) the date of importation, (2) the port of entry, (3) the description of the merchandise, (4) the quantity involved, (5) the name and address of the manufacturer, (6) the country of origin, (7) the name and address of the exporter, and (8) the name and address of the importer.[2] CBP officials also stated that CBP is only able to provide such information to specific entities, such as the rights holder and the importer of record. CBP officials noted that, if an e-commerce website is not listed as the importer on forms submitted to CBP, CBP cannot share information with that website. The officials were unable to specify whether these existing limitations are statutory or regulatory in nature.

Question. CBP is currently reviewing options for sharing additional information with rights holders and e-commerce websites. What is the timetable for this review?

Answer. In its official response to our report, CBP stated that it intended to complete its review by September 30, 2018. In responding to a question from Senator Wyden during the committee's March 6th hearing on this topic, a CBP official stated that CBP would attempt to accelerate this review, if possible.

Question. What are the differences between the information sharing rules for the CBP and ICE?

Answer. We did not evaluate the differences in information sharing rules between CBP and ICE. In the report, we noted that representatives of one e-commerce website stated that ICE sometimes shares information that is not shared by CBP, but ICE's involvement in the enforcement process begins only after CBP has identified and seized counterfeit items. CBP officials told us they have discussed differences in CBP's and ICE's information sharing practices with ICE officials to determine what information collection and sharing best practices could be used by CBP.

Question. How is the relationship with the Intellectual Property Center working? In your view, is CBP getting sufficient information to properly do the job?

Answer. We did not specifically evaluate the IPR Center's operations or its provision of information to CBP. However, we noted that collaboration between CBP and ICE—including at the IPR Center—is generally consistent with selected key practices for interagency collaboration. Additionally, some private sector representatives we spoke with praised the work of the IPR Center.

Question. CBP and ICE coordinate with several other Federal agencies in their efforts to interdict the flow of counterfeit goods into the United States. As a part of this effort, CBP and ICE also work with rights holders to ensure that their trademarks and copyrights are recorded in the CBP online system. Also, CBP puts a priority on enforcing IP registered with the U.S. Patent and Trademark Office and the U.S. Copyright Office.

According to the GAO report, increasing the number of patents, trademarks, and copyrights with the CBP was an important way that a rights holders can help CBP's enforcement efforts.

Given the benefits of registering patents, trademarks, and copyrights with CBP, does the U.S. Patent and Trademark Office or the U.S. Copyright Office share information with the CBP?

If so, what steps could be taken to improve the sharing of registrant information for new patents, trademarks and copyrights?

Could the U.S. Patent and Trademark Office or the U.S. Copyright Office forms be adapted to provide simultaneous registration with the CBP?

Answer. We did not review information sharing between CBP and the U.S. Patent and Trademark Office or the U.S. Copyright Office or ways to improve the process for recording IP with CBP. CBP officials noted that rights holders are often unaware of CBP's recordation process and that rights holders may not recognize that IP that is registered with the U.S. Patent and Trademark Office or the U.S. Copyright Office is not automatically recorded with CBP. We noted in our report that CBP prioritizes enforcement of IP that has been recorded with CBP after it has been registered with the U.S. Patent and Trademark Office or the U.S. Copyright Office. CBP engages in efforts to enhance awareness of this process, such as meeting with industry groups, according to CBP officials. Representatives of one rights holder told

[2] 19 CFR § 133.21.

us that increasing the number of trademarks recorded with CBP was an important component of the company's enhanced IPR enforcement efforts.

Question. Shopping online has changed immensely over the past couple decades. Consumers can buy almost anything online without having to leave their homes and receive it within a couple of days or quicker. Because the United States has changed the way it purchases its products, the chances of consumers unintentionally and unknowingly purchasing counterfeit products have increased. With worldwide e-commerce sales expected to reach nearly $4 trillion by 2020, this is an extremely pressing issue.

What were GAO's findings on how CBP is sharing information with e-commerce companies on seizures of counterfeits made at the U.S. border and ports of entry?

Was there specific information that you found that CBP could be sharing with e-commerce companies to help them locate and remove counterfeit items?

Do you think that consumers would benefit from CBP sharing this information with e-commerce companies to help stem the flow of counterfeits into the United States?

Answer. We found that CBP information sharing with e-commerce companies on counterfeit seizures is limited. According to CBP officials, CBP can only share information about seizures with specific parties, including the rights holder and the importer. CBP officials noted they are not permitted to share information with e-commerce websites if they are not listed as the importer on forms submitted to CBP. Representatives of two e-commerce websites stated that, because CBP does not inform them when seizures occur, they may not be aware of IPR-infringing goods offered for sale on their website even if CBP has seized related items from the same seller. Additionally, representatives of one website noted that information on the exterior of seized packages, such as business identifiers on packages destined for distribution centers, would be helpful for identifying groups of counterfeit merchandise from the same seller that may be housed in the distribution center and could be removed from commerce. As we noted in the report, the changing market for counterfeit goods poses a number of threats to consumers. Consequently, taking action to limit counterfeit sales and better protect IPR could benefit consumers. We recommended that CBP assess what, if any, additional information would be beneficial to share with the private sector and, as appropriate, take action to enhance information sharing such as by proposing regulatory changes or requesting additional legal authorities.

QUESTION SUBMITTED BY HON. BILL NELSON

Question. In GAO's report on counterfeit goods, it says "according to private-sector representatives we spoke to, restrictions on CBP's information sharing limit the ability of rights holders and e-commerce websites to protect IPR." The 2015 Customs bill (Pub. L. 114–125) was supposed to take care of the red tape on this, authorizing CBP to share information with intellectual property owners. Please explain why this problem still exists.

Answer. We note in the report that, in the Trade Facilitation and Trade Enforcement Act of 2015, Congress provided CBP with explicit authority to share certain information with rights holders prior to completing a seizure.[3] However, the private-sector entities we spoke with highlighted restrictions on CBP's information sharing after a seizure has been completed. Representatives of e-commerce websites noted they do not receive much information about completed seizures from CBP. According to CBP officials, CBP can only share information about seizures with specific parties, including the rights holder and the importer. CBP officials noted they are not permitted to share information with e-commerce websites if they are not listed as the importer on forms submitted to CBP. Representatives of two e-commerce websites stated that, because they do not regularly receive information from CBP, they may not be aware of IPR-infringing goods offered for sale on their website even if CBP has seized related items from the same seller.

Representatives from both rights holders and e-commerce websites noted that limitations on the specific pieces of information provided by CBP impede their ability to protect IPR. For example, one rights holder representative stated that the infor-

[3] This authority applies only with respect to goods suspected of infringing a trademark or copyright that is recorded with CBP. Pub. L. No. 114–125, § 302(a).

mation CBP provides, such as importer names from bills of lading, is sometimes not useful, because counterfeiters use fake identities or otherwise mask their identities. Another rights holder said that some European customs agencies are able to share more information than CBP, better enabling rights holders to take action following a seizure.[4] Additionally, representatives of one website noted that information not currently provided by CBP, such as business identifiers that are clearly visible on the exterior of seized packages destined for distribution centers, would be helpful for identifying groups of counterfeit merchandise from the same seller that may be housed in the distribution center and could be removed from commerce. However, as we noted in the report, CBP has not yet completed an assessment of additional information that would be beneficial to share with the private sector or determined whether it can share such information under current regulations and statutes. Consequently, we recommended that CBP conduct such an assessment and, as appropriate, take action to enhance information sharing such as by proposing regulatory changes or requesting additional legal authorities.

PREPARED STATEMENT OF HON. ORRIN G. HATCH,
A U.S. SENATOR FROM UTAH

WASHINGTON—Finance Committee Chairman Orrin Hatch (R–Utah) delivered the following opening statement at a Finance Committee hearing entitled, "Protecting E-commerce Consumers From Counterfeits."

I'd like to welcome everyone here today. During this hearing, we will discuss counterfeiting in e-commerce and what steps we can take to protect consumers.

Before we get to that though, I'd like to make an important point about the President's proposed tariffs on steel and aluminum.

Let's set aside, just for a moment, all of the legitimate concerns about trade wars, the failure to target the source of steel and aluminum overcapacity, and the disproportionate effects on our major trading partners and allies. In the end, these tariffs are not a tax on foreign steel and aluminum producers, but rather a tax on American citizens and businesses, who, if this action is finalized, will be forced to pay an additional 25 percent on steel and 10 percent on aluminum.

Those effects would blunt the benefits of tax reform for all Americans—including the reduced impact of the billions of dollars that many companies recently pledged to invest here in America.

And those billions would not be as valuable. Truly, there is a better way to address China's actions than to impose a new, across-the-board tax on U.S. consumers and businesses just 3 short months after we passed comprehensive tax reform. We can and should do better. And I will be sending the President a letter later today emphasizing just that.

Now, I'd like to turn to the important issues we want to address in this hearing.

It's no secret that I have long felt that strong protections for intellectual property rights protect consumers. A properly enforced trademark, for example, lets a customer know who made a product and where to go for information about it.

We were all encouraged by the new authorities the Trade Facilitation and Trade Enforcement Act of 2015, granted the U.S. Customs and Border Protection as well as Immigration and Customs Enforcement. Those authorities, along with the new National Intellectual Property Center, were designed help agencies collaborate, coordinate, and take down perpetrators.

Because there are frequently hiccups with the implementation of new laws, the committee asked the Government Accountability Office to conduct a broad investigation about how the Trade Facilitation and Trade Enforcement Act was being implemented.

As they started their investigation, GAO quickly began to realize that e-commerce, generally, was causing major issues for CBP and ICE. Due to advancements

---

[4] CBP officials noted that, with regard to an IPR seizure, CBP is legally allowed to share (1) the date of importation, (2) the port of entry, (3) the description of the merchandise, (4) the quantity involved, (5) the name and address of the manufacturer, (6) the country of origin, (7) the name and address of the exporter, and (8) the name and address of the importer. 19 CFR § 133.21.

in online purchasing, the agencies were being forced to adopt new tactics, work more closely together, and build up their public-private partnerships.

Those have all been changes for the good. However, we asked GAO to continue their investigation and to look specifically at the problem of counterfeits on some of the most prominent e-commerce platforms.

As part of this process, GAO made purchases from five major e-commerce platforms. And, after using relatively narrow criteria, GAO received at least one counterfeit and one legitimate good from each of the platforms. In the end, 20 of the 47 individual items they purchased were counterfeit.

While the sample size was small, the results are still telling. On the whole, this investigation started us down a path of discovery, and on that path we noticed there are far more issues than we had initially anticipated.

Today's hearing represents a culmination of those initial findings. And while we are not going to be able to fix this all at once, I am hoping to at least discuss some meaningful steps that we could take in the near term.

But, before we get to that, I want to talk a little bit more about what we found. As part of its research, GAO found that many counterfeit products create a hazard to consumers, children, and our economy. Through seizures and later investigations, CBP, ICE, and CPSC have found numerous instances of counterfeit products with major health and safety issues. These issues have included contact lenses that contain dangerous bacteria, cosmetics that have chemicals that can cause harmful health effects when applied, phone chargers with faulty wiring, batteries with thermal runoff issues, and even defective airbags.

GAO has found that with the rise of popular online marketplaces, counterfeiters have greater access to the market and can easily sell their phony products directly to consumers.

Because the counterfeiters frequently use stock photos, or simply join in on a prelisted product, the goods are sold as genuine, and so long as counterfeiters can make the products indistinguishable on the outside, most consumers never notice a difference. This is because typical red flags for consumers are difficult to notice. This is even true when the counterfeiters create new colors or designs of more famous products.

In one recent instance, the U.S. Attorney's office in the Northern District of Mississippi successfully prosecuted a case against Bobby Rodgers, Jr.

Mr. Rodgers had a fairly elaborate scheme in place. First, he would order counterfeit merchandise from China and facilitate delivery by using alternate addresses. Then, he would powder-coat the counterfeit items he received and sell them as a third-party retailer online. As he did this, he would represent the goods as authentic, sometimes even with licensed modifications.

The sheer volume of his scams was staggering. On just one of the two major platforms he used, Mr. Rodgers had sold over $300,000 in counterfeit goods. When his complex was raided authorities seized another 2,200 pieces of counterfeit drinkware.

But it doesn't end there.

Later, as the CPSC lab reports came back, several of the colors tested positively for lead, exceeding the amount legally allowed by more than 20 times. For all we know, there are currently children around the country sipping water with dangerously high levels of lead because of Mr. Rodgers.

Sadly, he is just one among many, many perpetrators buying counterfeits and facilitating sales of them through e-commerce platforms.

We've heard from some rights holders, like YETI, whose products have been counterfeited in these schemes, who have responded strongly to address these problems.

YETI issued a statement making it clear that they were expending "significant resources to protect [their] consumers." I ask unanimous consent that the full YETI statement, as well similar statements submitted by other rights holders, be entered into the appropriate place in the hearing record.

Now, I don't want to steal too much of their thunder, but one of the reasons we've invited Underwriters Laboratories, or UL, here today is to let them give us a broader perspective on the seriousness of these issues.

As just one example, in a public report, UL recently tested 400 counterfeit Apple Phone Adapters, out of those 400 they found that only 3 out of the 400 chargers passed electricity strength tests. And that is just one of the many studies UL has performed.

I think everyone here—both members and the audience—will be stunned by not only the breadth of products being counterfeited, but also by the incredible volume. This goes beyond the dollars and cents these companies have invested to develop and market their products, which, let's be clear, are enormously important for our economy, not to mention the well-being of American consumers.

But we're not just talking about devalued investments. We're talking about lead on children's drinkware, phones catching fire, homes burning down, consumers being injured from hygiene and cosmetic products, airbags not inflating properly, and who knows what else.

It is my hope that we all can all agree today that counterfeit products pose an immediate and significant risk to Americans' health and safety. And I hope that we can take GAO's recommendations seriously to improve information sharing and better track CBP's intellectual property enforcement methods.

Personally, I am interested in talking specifically about sharing e-commerce platform data contained in invoices and on packages with rights holders, as well as learning from and improving CBP's voluntary abandonment program.

American consumers are relying on us to get this right, and we need to work together and with the appropriate officers at CBP, ICE, and other agencies to make sure we do.

YETI
7601 Southwest Parkway
Austin, TX 78735
512–394–9384

March 2, 2018

U.S. Senate
Committee on Finance
Dirksen Senate Office Building
Washington, DC 20510–6200

Re: Senate Finance Committee Hearing, "Protecting E-commerce Consumers From Counterfeits," March 6, 2018 at 10:00 AM

Dear Chairman Hatch, Ranking Member Wyden, and all Members of the Committee:

The increasing prevalence of counterfeit goods in the U.S. economy is both alarming and concerning. Counterfeiting is a growing, global craft of well-funded criminals that threatens consumer safety, undermines consumer confidence and erodes the reputation of innovative companies.

As a target of counterfeit activity, YETI has expended significant resources to protect our consumers, our intellectual property rights and our brand from the actions of both counterfeiters and those who facilitate the importation and sale of counterfeits, including E commerce marketplaces based in the United States and abroad. The recent report issued by the Government Accountability Office, "Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market," helps shine a light on the role that online marketplace platforms play in the trafficking of counterfeit goods.

We commend the GAO for investigating this critically important issue and thank Chairman Hatch, Ranking Member Wyden and the Senate Finance Committee for hosting this hearing.

Thank you for your consideration of this submission for inclusion into the hearing record. If you or your staff have any questions regarding this letter, please feel free to contact me.

Matthew J. Reintjes
Chief Executive Officer

BELKIN INTERNATIONAL
12045 East Waterfront Drive
Playa Vista, CA 90094
Office: +1 310–751–5100
Fax: +1 310–751–5969

March 6, 2018

Hon. Orrin Hatch, Chairman
U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

Hon. Ron Wyden, Ranking Member
U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

Re: Statement for the Record, "Protecting E-commerce Consumers From Counterfeits"

Dear Chairman Hatch and Ranking Member Wyden:

As the chief legal officer and general counsel of Belkin International and previous Finance Committee witness on the challenges to U.S. businesses in the digital age, I am pleased to see the committee's continued focus on the need to protect consumers from counterfeit products. Today, Belkin has over 1,300 employees in over 25 countries, with more than 750 in the United States. As I noted in my testimony before the committee in June 2016, the digital age has ushered in a new era of previously unimaginable opportunities, as well as significant challenges for both companies and consumers. I welcome the opportunity to update the committee on Belkin's progress and ongoing challenges since our 2016 testimony.

Belkin celebrates the digital age. Since its inception, Belkin has sought to give consumers peace of mind and make their lives better, easier, and more fulfilling. The Belkin mission is to create people inspired products, and the first step in doing so is understanding what consumer needs are and predicting what they will be. Belkin is committed to creating the highest quality authentic products and actively works to educate our consumers and identify and dismantle counterfeit operations using a multi-pronged approach. Our extensive brand protection program leverages the strong relationships that we have established with governments, regulators, distribution networks and anti-counterfeiting organizations worldwide.

Belkin believes in the digital marketplace, the value of global e-commerce, and its importance to Belkin and American job growth. Like our peer companies, we advocate for a level playing field, and believe that, with fair competition, we and other American companies will succeed in that competition by working harder and with more innovation than our competitors abroad. This committee's continued work to address counterfeiting draws needed attention to intellectual property rights enforcement that is key to the success of both American companies, of all sizes, and the American economy.

The Belkin brand protection team (BPT) is an efficient and effective team. In addition to monitoring physical marketplaces and supply chains, Belkin continually sweeps key online marketplaces to find and remove brand-infringing listings. Since 2016, we have removed 2.7M brand infringing products worldwide. When we find evidence of extensive counterfeiting activity by a distributor or manufacturer abroad, we conduct private investigations and then work with local law enforcement authorities to take action. In addition, the BPT organizes training to customs authorities across the globe, including in Asia, Europe, the Middle East, and the Americas, to help customs agents identify potential counterfeit products at their borders. Belkin has also taken private legal action in numerous countries across the globe against entities that violate our intellectual property rights, all in an effort to thwart the sale of unlawful and potentially unsafe products.

As detailed in my 2016 testimony, Belkin encountered copycat products in China marketed under the brand name "Melkin." Melkin products replicated Belkin's trade dress, and were branded with the express purpose of confusing consumers into thinking that they were purchasing Belkin products. This company, and the individuals and entities behind it, benefited unfairly from the Belkin name and reputation while causing significant harm to our business and to consumers. As of February

2017, we successfully opposed registration of the Melkin trademark in more than 20 countries, including China, removed Melkin products from major e-commerce sites, and got an injunction to prevent Melkin-branded products to be sold in Hong Kong.

While Belkin has the tools and resources to engage in these global efforts to defend our products and brand, many small businesses do not. The livelihoods and reputations of U.S. small businesses and startups are similarly threatened by counterfeit products, so it is imperative that the Federal Government continues its intellectual property enforcement efforts to bolster private-sector resources.

Counterfeits also threaten the security of our supply chain. Whether contributing to Federal IT systems, military equipment, or consumer products and services, many companies supply the components to a final product. This complexity creates multiple entry points for counterfeit materials to enter the U.S. supply chain, creating security challenges for the military, government, and consumers, as they create and use innovative products and services to protect critical infrastructure, national security, and personal identities.

Public safety is another important issue that is raised by proliferation of illegal counterfeit products. Genuine Belkin products have undergone rigorous safety certifications, testing, and protocols. Counterfeiters and copycats simply have no concern for quality and safety. At Belkin, we are dedicated to our consumers' safety and enjoyment while using our products, and so design and quality informs everything that we do, from our user testing and prototyping process, to strict adherence to regulatory compliance, manufacturing, and warranty programs. Rigorous enforcement of counterfeiting laws and aggressive work with our international partners is necessary to stem the flow of unsafe counterfeit products.

Thank you for the opportunity to submit Belkin's views on protecting consumers and the Federal Government from illegal counterfeiting activities. We look forward to continued engagement with the Finance Committee on this issue. Please let me know how Belkin may be of further assistance in your efforts.

Sincerely,

D. Thomas Triggs
Chief Legal Officer and General Counsel
Belkin International, Inc.

THE INTERNATIONAL ANTICOUNTERFEITING COALITION, INC.
727 15th Street, NW, 9th Floor
Washington, DC 20005
+1 (202) 223–6667
iacc@iacc.org
www.iacc.org

Chairman Hatch, Ranking Member Wyden, and Members of the Committee:

The International AntiCounterfeiting Coalition ("IACC") is pleased to offer this written statement for the record in connection with your March 6, 2018, hearing concerning, "Protecting E-Commerce Consumers From Counterfeits," and we thank you for examining this important topic. We are available at your convenience to discuss any questions you might have regarding these comments or to otherwise provide clarification of our submission.

With a membership composed of approximately 250 corporations, trade associations, and professional firms, and founded nearly 40 years ago, the International AntiCounterfeiting Coalition ("IACC") is the world's oldest and largest organization devoted solely to combating product counterfeiting and piracy. The members of the IACC represent a broad cross-section of industries and include many of the world's best-known companies in the apparel and luxury goods, automotive, software, personal care, electronics, consumer goods, entertainment, pharmaceutical, and other product sectors. The IACC is committed to working with government and industry partners in the United States and abroad to strengthen IP protection and enforcement, and to raise awareness regarding the range of harms caused by counterfeiting and piracy.

The comments provided herein highlight the challenges faced by both rights holders and our government partners in the enforcement of intellectual property rights, in the current e-commerce landscape. We are also pleased to share information regarding our ongoing collaborative efforts that seek to address these concerns, and to

offer our thoughts on additional steps which could help to safeguard consumers and legitimate businesses in the online ecosystem. We look forward to working with the Committee on these issues.

Evolving Distribution Models

Historically, the distribution chains for counterfeit goods have largely mirrored those of legitimate commerce. It should come as no surprise then that China, the largest source of consumer goods imported into the United States, has also been the greatest source of counterfeit goods arriving at our borders for a number of years. In Fiscal Year 2017, the People's Republic of China was cited as the country of origin for 48 percent of all seizures effected by U.S. Customs and Border Protection ("CBP") (16.5K out of more than 34.1K total seizures), and 46 percent by value ($554.63 million out of a total of $1.2 billion).[1] It is worth noting, however, that Chinese imports actually account for a much larger percentage of CBP's seizures than the raw figures would indicate. The second position on CBP's list is occupied by Hong Kong, identified as the source country of 39 percent of seizures (32 percent by value). Hong Kong though is not widely viewed as a manufacturing hub for counterfeit goods, but rather as a major transshipment point for counterfeits produced by mainland China.

Until relatively recently, ocean-going container vessels have played the most significant role in facilitating these illicit imports. Counterfeiters have exploited cheap labor and lax enforcement regimes abroad to manufacture low-cost knock-offs to supply domestic wholesale and distributor networks in the United States, which in turn have fed the retail market for counterfeits. This so-called "brick-and-mortar supply chain" centered largely around flea markets, swap meets, and small storefronts in well-established hot-spots in major metropolitan areas such as New York's Canal Street area and Santee Alley in Los Angeles. In more recent years however, we've seen a drastic shift in the ways counterfeit goods travel from the point of manufacture to the end consumers. Concurrent with the rise of online shopping and the development of e-commerce platforms, we've seen a steady increase in the volume of counterfeit seizures by CBP in the express consignment and postal shipping environments. As detailed in CBP's above-referenced report, these small consignments accounted for 89 percent of seized shipments, and 47 percent of total seizures by value.

This shift is no doubt partly due to the concerted efforts of both law enforcement and rights holders in investigating and prosecuting sales and distribution networks throughout the United States. Further, it is indicative of the increasing sophistication of counterfeiters' operations, including their exploitation of e-commerce services and other providers to directly target and sell to consumers. This evolving distribution model bypasses a number of the traditional opportunities for enforcement available to rights holders and law enforcement personnel, while both are necessitating the application for ever greater enforcement resources for ever-diminishing returns. While the border enforcement of IP rights was often characterized in the past as searching for a needle in a haystack, the explosion in small parcel shipments has served to shrink the proverbial needle while exponentially increasing the number of haystacks. And while in the past, a single seizure of one or more containers might substantially decrease the availability of counterfeits in the market and significantly impact a counterfeiter's bottom line, achieving that same impact requires the seizure of thousands of small parcels. Understanding how the trafficking of counterfeit goods has evolved and developing new strategies to attack this illicit trade is vital to protecting U.S. consumers and businesses in the current environment.

Existing Efforts to Combat the Trafficking of Counterfeit Goods in E-Commerce

As rights holders and others have sought to address the trafficking of counterfeit goods online, a great deal of attention has been placed on the so-called "choke points" in the e-commerce ecosystem. We must take into account how counterfeiters are reaching their customers, how the goods are purchased and sold, and how the goods are getting from the seller to the buyer. Each step in the distribution chain presents an opportunity for rights holders, enforcement personnel, and other responsible parties to disrupt the counterfeiters' illegal businesses; the IACC has been a leader in the development of voluntary collaborative agreements with stakeholders from a variety of industry sectors to achieve that goal. Our RogueBlock®[2] and IACC

[1] "Intellectual Property Rights Seizure Statistics—Fiscal Year 2017," *https://www.cbp.gov/sites/default/files/assets/documents/2018-Feb/trade-fy2017-ipr-seizures.pdf.*

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

MarketSafe®[3] programs offer examples of the positive impact that such collaboration can have in targeting two of the above-mentioned choke points in the modern distribution chain—the online storefront where items are displayed to potential buyers, and the payment mechanism.

The IACC launched its RogueBlock® program in January 2012 as a means to providing a streamlined, simplified procedure by which rights holders could report online sellers of counterfeit or pirated goods directly to participating credit card and payment processing network partners. This effectively facilitated action against the merchant accounts associated with those websites and diminished the ability of individuals to profit from their illicit sales. The program has seen great success, and significant expansion over the past 3 years, and has been viewed as a "win-win" for all of the parties involved. Rights holders are able to provide timely, relevant intelligence, and in the process aid financial service providers in policing bad actors who seek to misuse legitimate commercial tools for illegitimate purposes.

Our goals upon commencing the RogueBlock program were: (1) to increase the cost of doing business for, and decrease profits to, the counterfeiters; (2) to shrink the universe of third-party acquiring banks willing to do business with rogue merchants; (3) to facilitate an efficient use of resources by both IP owners and our partners by sharing relevant data and avoiding the duplication of efforts; and (4) to disrupt and dismantle counterfeit networks. By any measure, we are achieving those goals. Equally important, the strong partnerships we've developed in the financial sector are enabling us to continue enhancing, expanding, and evolving to face new challenges in the online space. To date, our collaborative efforts with the payment sector have resulted in the termination of over 5,300 merchant accounts in connection with the illegal sale of counterfeit goods online. By conservative estimates, upwards of 200,000 websites have been deprived of the means to accept payment for their illegal products.

As was made clear by the recently published report by the Government Accountability Office,[4] counterfeit sellers are increasingly seeking to exploit legitimate e-commerce services to reach unwitting consumers. Online marketplaces are attractive targets for counterfeiters—consumers' familiarity with the platforms, and the goodwill and trust imbued by that familiarity, typically extends to the individual sellers on the platform. As a result, counterfeiters need not seek out and attract consumers themselves; by infiltrating a well-known marketplace, the consumers will come to them.

Recognizing this concern, the IACC has worked closely with partners in that sector to identify and target those counterfeiters seeking to exploit the consumer markets represented by platform sites. Beginning in 2014, our IACC MarketSafe program, developed in cooperation with the Alibaba Group, has succeeded in removing over 300,000 listings, and has resulted in more than 7,000 sellers of counterfeits being permanently banned from the Alibaba platforms. In 2017, that program was expanded to enable greater participation by rights holders—including non-IACC members. Importantly, the expanded program has been offered to rights holders at no cost, facilitating participation by SMEs that may lack the resources available to larger companies. More recently, the IACC and its members have been working with Amazon on voluntary efforts to fight counterfeits; later this year, we'll launch a new pilot initiative to strengthen our collaboration with Amazon, with the aim of enhancing cooperative industry efforts to stop IPR infringement. Similarly, we are seeking to engage more closely with other major platforms including eBay, and other potential partners, to ensure the safety of consumers online.

In addition to such private-sector collaborations, the IACC has long-recognized that our partners at U.S. Customs and Border Protection are our nation's front-line defense against illicit counterfeit goods. Throughout 2017, the IACC hosted 23 training seminars for Customs personnel, as well as Federal, State, and local law enforcement officials around the United States, including at some of the highest priority ports of entry for intellectual property enforcement. Those programs will remain a cornerstone of our engagement with enforcement personnel in the coming year, along with our continuing work with the National IPR Coordination Center, and the Department of Justice's Computer-Crime and Intellectual Property Section (CCIPS).

We are cognizant of the fact however that the challenges faced by rights holders and law enforcement do not stop at our own borders. Accordingly, we are actively work-

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

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

ing to aid in the development of truly global partnerships among relevant stakeholders. To that end, the IACC, in collaboration with UL, co-hosted major international conferences last year with EUROPOL in Antwerp, and with INTERPOL in New York. In 2018, we will build on the success of those events with conferences in Budapest and Dubai, drawing rights holders, law enforcement, and intermediaries from around the globe. In addition, the IACC hosted training seminars last year in Colombia, Mexico, and the Dominican Republic, and will host our second Latin America Regional Brand Protection Summit this October, bringing together representatives from over a dozen trading partners in the region. We also continue to work closely with the National IPR Coordination Center here at home, and to support the work of the U.S. Patent and Trademark Office's international IP attaches, as well as USPTO's Global IP Academy.

Our member companies invest heavily to keep dangerous counterfeits out of consumers' hands. They spend countless hours and millions of dollars each year to develop and incorporate new technologies into their products and packaging to thwart counterfeiters' attempts to defraud consumers, to investigate violations of their rights and seek civil and criminal enforcement, and to offer investigative and prosecution support to our colleagues in the public sector. But they also understand that counterfeiting is a problem far larger than any of them can handle alone. The IACC recognizes that collaboration both within the private sector and between the public and private sectors is essential to protect consumers from often dangerous counterfeit goods, and to further protect legitimate businesses and the U.S. economy from the unfair competition represented by the trade in counterfeits.

Opportunities for Increased Collaboration to Combat Counterfeits

Our success or failure in the fight against counterfeiting online ultimately relies on the ability and willingness of all responsible stakeholders in the e-commerce landscape to identify and weed out bad actors within the system. To do so will require robust collaboration among all of the relevant parties to develop and share intelligence about illegal activity when it has been identified, and a commitment to acting upon that intelligence. This model has served as the basis for rights holders' interactions with CBP and other law enforcement agencies for countless years and has been underscored by recent Congressional action. Included below are recommendations to enhance such collaboration, which we believe are essential to more effectively combat the trafficking of counterfeits online.

Historically, intellectual property owners, including IACC members such as L'Oréal and UL, among others, have provided invaluable assistance such as technical support and expertise to those CBP personnel tasked with the enforcement of IPR at our Nation's borders. This assistance has been necessitated by a number of factors, including the overall volume of imports passing through U.S. ports, the variety of goods presented to CBP for inspection, and more recently, the increasing ability of counterfeiters to manufacture more convincing fakes. Legitimate manufacturers have traditionally aided CBP with product authentication through the examination of suspect items, and by providing a range of information related to the sourcing and distribution chains for their legitimate goods. In turn, the owners of trademarks and copyrights recorded with CBP are provided a variety of information gleaned from Customs' detentions and seizures of shipments in violation of those rights. The mutual exchange of information drives CBP's targeting of shipments, the government's criminal investigations, and rights holders' private investigations and civil actions to enforce their rights.

In more recent years, however, such sharing of information has been constrained because of concerns raised by CBP regarding its legal authority to share certain information, or to seek rights holders' assistance, particularly in advance of a formal detention or seizure action. Congress appeared to have addressed those concerns with its inclusion of provisions in the National Defense Authorization Act for Fiscal Year 2012,[5] and provided further clarification of its intent as set forth in section 302 of the Trade Facilitation and Trade Enforcement Act. Prompt implementation

[5] Section 818(g)(1) reads, "If United States Customs and Border Protection suspects a product of being imported in violation of section 42 of the Lanham Act, and subject to any applicable bonding requirements, the Secretary of the Treasury may share information appearing on, and unredacted samples of, products and their packaging and labels, or photographs of such products, packaging, and labels, with the rights holder of the trademarks suspected of being copied or simulated for purposes of determining whether the products are prohibited from importation pursuant to such section."

of that authority would be welcomed to encourage a more free-flowing exchange of intelligence between CBP and its private-sector partners.

Similarly relevant, in the context of e-commerce, is the implementation of CBP's Voluntary Abandonment procedures. Initially developed as a pilot program to facilitate the efficient processing of small consignments of suspected counterfeit goods, CBP has expressed reluctance to share information with stakeholders concerning the shipments interdicted under those procedures, noting that such disclosures are authorized by regulation only where goods have been detained or seized. We have recently learned that this pilot program has been concluded, and that direction to the ports will be forthcoming regarding broad implementation. While we recognize that such procedures could be a valuable enforcement tool, given the fact that 89 percent of FY2017 seizures involved express consignments or international mail shipments, it is vital that CBP both captures and shares relevant data from those shipments whether they're interdicted via the abandonment or seizure processes. Such intelligence is vital to rights holders' own investigations and efforts at self-help, and to their ability to provide further support for targeting and criminal enforcement actions by their law enforcement partners. To that end, we ask that the Committee provide any requisite clarification of CBP's authority to share relevant data with their partners in the private sector, and if necessary, to enact legislation clearly authorizing such disclosures.

We commend CBP for its efforts at engaging the express consignment sector on this initiative, and its recognition that shipping intermediaries—whether in the private sector or in the public mail service—have a role to play in protecting consumers from counterfeits. Accordingly, we are also supportive of ongoing initiatives to facilitate the provision to CBP of advance electronic data for international mail shipments, akin to the data provided by private carriers. Such disclosures would no doubt aid in CBP's dual mission of facilitating legitimate imports and enforcing against illicit imports.

Consumer safety must be a priority for every responsible participant in the e-commerce marketplace. We welcome the Committee's leadership in highlighting these important issues, in recognizing the work currently being done, and for underscoring the importance of meaningful collaboration among stakeholders across all of the relevant sectors and our partners in enforcement. The IACC looks forward to working with you to ensure that the online marketplace continues to grow as a trusted and reliable outlet for consumers and legitimate businesses.

I thank you for your consideration of these comments, and I would welcome the opportunity to discuss these matters further with the committee.

Respectfully submitted,

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

FOOTWEAR DISTRIBUTORS AND RETAILERS OF AMERICA (FDRA)

On behalf of the Footwear Distributors and Retailers of America (FDRA), we appreciate the opportunity to provide written testimony to the Senate Finance Committee for its recent hearing on protecting e-commerce consumers from counterfeits.

Founded in 1944, FDRA is governed and directed by U.S. footwear executives and remains the only U.S. trade association dedicated solely to footwear. FDRA serves the full footwear supply chain, from design and development to manufacturing to distribution and retail. Members range from small, family-owned businesses to global brands that sell to consumers around the world. Today, FDRA supports nearly 500 companies and brands, including the majority of U.S. footwear manufacturers.

FDRA greatly appreciates the work the Committee has done to address the troubling and rapidly expanding problem of counterfeiting in markets around the world. The Trade Facilitation and Trade Enforcement Act (TFTE Act), in particular, sharpens the tools and processes we have for addressing intellectual property rights (IPR) challenges. In addition, we applaud the Committee for initiating the Government Accountability Office (GAO) review of current IPR enforcement at U.S. borders, which is the focus of this hearing.

Strengthening IPR enforcement has become one of the top priorities for the U.S. footwear industry. FDRA member companies work hard to design, produce, and deliver over 2.3 billion pairs of shoes to U.S. consumers each year, and many of our

members also sell brands that reach consumers in markets all over the world. These companies manage supply chains that span the globe, providing them with hands-on familiarity of the significance of intellectual property (IP) and innovation. Attention to these issues supports U.S. footwear jobs and communities nationwide. Protecting IP remains vitally important to our industry, as our members continue to incorporate cutting-edge designs and technology into their products.

The findings of the GAO report are extremely concerning for the U.S. footwear industry. Of the 47 items GAO purchased from third-party sellers on popular e-commerce platforms, 20 turned out to be counterfeit products. In fact, every one of these platforms selected by GAO yielded at least one counterfeit item in connection with this study. This has become such a problem for the footwear industry, that Birkenstock made headlines in 2016 and 2017 when it pulled all of its products from Amazon in both the U.S. and Europe, citing concerns about counterfeit sales on the platform.

In fact, the World Customs Organization's (WCO's) 2016 Illicit Trade Report found that an astounding 35.8 percent of worldwide seizures involved the confiscation of clothing, footwear, and textiles other than clothing.[1] According to the WCO, many of the leading footwear brands are among the most counterfeited brands in the world.[2]

While this unprecedented growth of e-commerce has dramatically increased choice for consumers and given U.S. footwear businesses new tools and channels to reach those consumers, it has created countless new opportunities for bad actors. To address these issues, we must ensure companies have greater resources to reduce the unauthorized sale of IP-protected products and that there is increased cooperation and collaboration between government authorities, platforms, and rights holders.

When Customs and Border Protection (Customs) seizes counterfeit products and alerts the rights holders, many cases never go further than the seizure of the product because of a lack of information. Additional information and processes for better information sharing could help track the real importer, increase enforcement actions, and reduce repeat counterfeit sellers and shippers.

FDRA members wish to provide the following list of concerns as you explore more effective ways in which to combat counterfeiting activities on e-commerce platforms:

1. Infringers increasingly ship tags and labels separately and attach them to the counterfeit product in the U.S., in order to avoid seizure by Customs. In many instances, Customs officials are either not willing or not trained to consider trade dress or design patent infringement as a basis for seizure.

2. Often, penalties are inadequate to deter criminal enterprises from engaging in trademark counterfeiting operations. In many countries, the penalties imposed for trademark counterfeiting operations are so low that they only add to the cost of doing business.

3. Infringers often use express mail and postal services to deliver counterfeit goods in small packages, making it more challenging for enforcement officials to confiscate these goods. The sheer volume of small shipments makes it impossible for CBP to adequately screen or x-ray all incoming mail to detect such shipments.

4. In numerous countries, there are legal and procedural obstacles to securing and enforcing trademark rights. Judicial systems in developing nations, for example, may lack transparency and independence, making it difficult for rights holders to pursue claims.

5. Counterfeiters now commonly register domains that advertise and sell counterfeit goods. Many of these counterfeiters use a country code top-level domain (ccTLD) to avoid detection and to avoid the reach of the U.S. judicial system. FDRA member companies face significant trademark infringement and lose valuable Internet traffic because of misleading and fraudulent domain names. It can be hard for companies to find redress, because a number of foreign reg-

---

[1] *See* World Customs Organization "Illicit Trade Report 2016" at page 140 (report found here: *http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/illicit-trade-report/itr_2016_en.pdf?db=web*).

[2] *See* World Customs Organization "Illicit Trade Report 2015" at page 78 (report found here: *http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/illicit-trade-report/itr_2015_en.pdf?db=web*).

istries do not make registration information publicly available and do little to assist aggrieved rights holders.

FDRA is an active participant in the annual Special 301 Review conducted by the Office of the United States Trade Representative (USTR). We have communicated these same concerns with officials across the various agencies entrusted to combat and protect U.S. intellectual property. We stand ready and willing to work with the Committee and the appropriate Federal agencies working on this vitally important issue.

Respectfully submitted,

Matt Priest
President and CEO

PREPARED STATEMENT OF JIM JOHOLSKE, DIRECTOR, OFFICE OF IMPORT SURVEILLANCE, CONSUMER PRODUCT SAFETY COMMISSION

Chairman Hatch, Ranking Member Wyden, and distinguished members of the committee, thank you for inviting me to discuss the U.S. Consumer Product Safety Commission's (CPSC) important role in protecting consumers from health and safety hazards involving imports and counterfeit goods. Before I begin, I should note that these comments are those of CPSC staff, and they have not been reviewed or approved by, and may not necessarily reflect the views of, the Commission. I especially appreciate the opportunity to appear before you today, as this year marks the 10th anniversary of the creation of CPSC's import surveillance program.

The CPSC was established by Congress in 1972, and is the Federal regulatory body charged with protecting the public from unreasonable risk of injuries or death associated with consumer products. We are a relatively small agency, with 545 full-time equivalents, and a $125 million annual budget. However, we have jurisdiction over thousands of consumer products, a vast majority of which are imported into the United States. I joined CPSC's Office of Import Surveillance when it was created in 2008, and I became its Director in March 2017. Before that time, I spent 8 years in the agency's Office of Compliance and Field Operations, where I worked on enforcement of mandatory regulations governing products under CPSC's jurisdiction. Our Office of Compliance and Field Operations performs a vital role within the agency, by investigating incidents involving consumer products and working with importers and manufacturers to implement recalls, if necessary.

Since passage of the Consumer Product Safety Improvement Act of 2008, CPSC has strengthened its relationship with U.S. Customs and Border Protection (CBP) and closely coordinates with CBP to interdict potentially noncompliant, unsafe imported products. As part of our efforts, CPSC has placed investigators at the largest ports of entry to work side-by-side with CBP staff. Currently, we have 30 investigators stationed at 20 of the largest ports in the country. Despite our relatively small size, in fiscal year 2017, CPSC investigators at the ports screened more than 38,000 distinct products arriving in the United States, and stopped approximately 4 million noncompliant or hazardous units from reaching consumers.

To prioritize and target high-risk shipments, CPSC has developed our own targeting system, called RAM or "Risk Assessment Methodology." RAM leverages a feed of entry data received from CBP, which is combined with CPSC data to risk-score shipments under CPSC's jurisdiction. We also have CPSC staff stationed at CBP's Commercial Targeting and Analysis Center (CTAC) to coordinate with CBP and other government agencies to address import safety issues through commercial trade targeting. At CTAC, we implement our national targeting programs using CBP's Automated Targeting System to identify potentially violative shipments. CPSC also has a part-time presence at the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) National Intellectual Property Rights Coordination Center (IPR Center). At the IPR Center, we are able to exchange information with 22 partner agencies that may help us target potentially non-complying and hazardous products. As an agency with limited resources, we would not be able to do the critical work of intercepting high-risk products before they reach consumers without the assistance and support of DHS and CBP.

Although CPSC's primary focus is targeting products that violate CPSC requirements, we do encounter Intellectual Property Rights (IPR) violations. As part of the work done at CTAC, CBP and CPSC staff target entities in the supply chain that are known IPR violators for possible health and safety issues. Many of CPSC's in-

vestigators are former CBP officers and import specialists and have been trained to identify IPR issues. CPSC investigators have also attended CBP's IPR Instructor-Led and rights-holder training at several ports, which has led to greater interagency referrals and collaboration. Consequently, although not our primary focus, CPSC staff is often able to identify possible IPR violations in the course of their normal duties.

When CPSC identifies a potential IPR issue, we refer the shipment to CBP because they have authority to efficiently seize the products. On a case-by-case basis, we will also test products that are IPR violative for compliance with CPSC mandatory safety standards, or to determine whether they are otherwise hazardous.

A recent example of our successful partnership is illustrated by a shipment of counterfeit toys seized by CBP in January at the Port of Los Angeles. As a result of CPSC and CBP's collaboration, CTAC identified a high-risk shipment from China, imported by a manufacturer that previously attempted to import noncompliant products. CTAC flagged the shipment, which was then examined by CBP and CPSC, and found that it contained toys bearing counterfeit trademarks of popular children's toys. CPSC determined that the products also contained excessive lead and small parts, in violation of CPSC regulations and the Federal Hazardous Substance Act. This coordination between our agencies resulted in the confiscation of nearly 2,800 unsafe and fraudulent toys at the port, keeping them from reaching America's children.

CPSC and CBP have similarly collaborated on many other shipments where a potential IPR violation and a safety violation were found. Examples include: holiday lights, cell phone wall chargers, lithium-ion batteries used in hoverboards, laptops, and cellphones, children's backpacks, and numerous toys.

Although CPSC's import surveillance activities have prioritized large ports of entry, like many agencies, we are facing challenges in regulating products imported through direct-to-consumer sales over e-commerce platforms. The volume of these shipments, and the limited amount of data required when the shipment arrives in the United States make targeting difficult. With CPSC's small size and limited resources, we currently do not have investigators stationed at locations where these small packages arrive, other than at one location at JFK airport. However, CPSC will continue to evaluate its staffing model to identify efficient ways to target and examine potentially unsafe products shipped directly to e-commerce consumers.

Thank you for the opportunity to share my remarks. I am happy to answer any questions you may have.

QUESTIONS SUBMITTED FOR THE RECORD TO JIM JOHOLSKE

QUESTION SUBMITTED BY HON. ORRIN G. HATCH

Question. Can you please explain your work at the National IPR Center, and further explain how can your work with CBP and ICE can be improved?

Answer. CPSC is one of the 23 partner agencies at the National Intellectual Property Rights Coordination Center. The Center is a valuable avenue for us to share leads, deconflict cases, and network with other Federal agencies, foreign governments, and industry stakeholders. CPSC has a part-time presence at the Center, and our liaison participates in staff and working group meetings, as well as outreach and training events for government groups and private industry.

CPSC has a strong partnership with CBP and ICE, including our co-location alongside CBP at some of the Nation's largest ports of entry and coordination on a daily basis to target and examine high-risk shipments. Our work with CBP and other partner agencies also occurs through our participation at the Commercial Targeting and Analysis Center (CTAC). We will continue to collaborate closely with those DHS agencies, particularly to address the challenge of e-commerce and direct-to-consumer shipments.

QUESTION SUBMITTED BY HON. RON WYDEN

Question. In one way or another, you all touched on the shift from containerized shipping to small packages. You have also highlighted the challenges in enforcement against counterfeit goods.

Given that we seem to be in a new era of trade, wouldn't you agree that the Federal government's enforcement strategy to go after counterfeit goods needs to adapt to the changing market? If so, what changes would you recommend in current CBP and ICE enforcement priorities and approaches?

Answer. The dramatic increase in e-commerce and direct-to-consumer shipments has created challenges for all Federal agencies that work to interdict counterfeit and noncomplying products at the border. In CPSC's experience working with CBP at the ports, CBP emphasizes targeting and enforcement of shipments containing counterfeit goods. Although CPSC's primary focus is targeting products that violate CPSC requirements, we do encounter counterfeit goods in our normal course of business and refer those shipments to CBP for appropriate action. CPSC's import surveillance activities have focused resources on large ports of entry. With CPSC's small size and limited resources, we currently do not have investigators stationed at locations where the vast majority of small packages arrive. In addition, the sheer volume of these shipments and the limited amount of data required when they arrive in the United States makes targeting difficult. CPSC will continue to evaluate its staffing model and attempt to identify efficient ways to target and examine potentially unsafe products shipped directly to e-commerce consumers.

QUESTION SUBMITTED BY HON. PAT ROBERTS

Question. The GAO study on how agencies can improve efforts to address risks posed by changing counterfeit markets found growth in e-commerce has attributed to counterfeiters producing a wider variety of goods sold on popular websites alongside authentic goods. The goods are often deceiving to consumers, due to counterfeiters gaining an appearance of legitimacy on third-party online marketplaces. What tools are readily available to empower consumers to make educated decisions when purchasing from third party sellers on e-commerce platforms?

Answer. The GAO report provided helpful advice for consumers to follow to try and limit the risks of buying counterfeit products online (Appendix II: Consumer Information and Advice for Avoiding Counterfeits Online, p. 47). CPSC would also recommend that consumers research CPSC recalls online at *www.cpsc.gov,* report unsafe products and research products at *www.saferproducts.gov,* and read available reviews of products and third party vendors.

QUESTIONS SUBMITTED BY HON. JOHN THUNE

DIRECT-TO-CONSUMER SALES OVER E-COMMERCE PLATFORMS

Question. Mr. Joholske, as chairman of the Senate Commerce Committee, which has jurisdiction over the CPSC, I would like to note Acting Chairman Buerkle's strong leadership over the agency and to reiterate my hope that she will be re-confirmed to a full term as chairman.

While CPSC has had some success interdicting dangerous products that are shipped through traditional channels, it appears that a major blind spot exists with respect to direct-to-consumer sales over e-commerce platforms.

What additional data would CPSC need to improve its targeting efforts with respect to these shipments?

Answer. Most direct-to-consumer sales over e-commerce platforms enter the country as *de minimis* shipments valued under $800. A *de minimis* shipment, commonly referred to as a section 321, is cleared based on manifest data, meaning it may be imported without filing formal entry and with fewer associated data elements. Notably absent are a formal entry number, a 10-digit Harmonized Tariff Schedule (HTS) code identifying the commodity, and an official importer of record or responsible party—upon which CPSC's current Risk Assessment Methodology depends. Access to manifest data, or a few key data elements, such as a responsible domestic entity, foreign manufacturer, and product identifier, would improve CPSC's targeting efforts for these shipments.

IMPROVED COORDINATION BETWEEN CBP, ICE, AND CPSC

Question. You noted in your testimony the current interaction between the CPSC and CBP and ICE. While each of your agencies has specific responsibilities within

your areas of jurisdiction, there are overlaps, especially with respect to ensuring consumer safety.

Are there existing statutory barriers that we need to address to improve the coordination among your agencies while continuing to use taxpayer dollars efficiently and avoid duplication of efforts?

Answer. Coordination could be improved if additional data elements were available for *de minimis* shipments, and if CBP was authorized to share that trade information with CPSC. Without an HTS code, CBP is unable to determine the requirements of partner government agencies, such as CPSC. Therefore, CBP cannot identify which shipments are under CPSC's jurisdiction or share information with our agency.

CPSC has a strong working relationship with CBP at ports of entry where we are co-located. However, with CPSC's small size and limited resources, we currently do not have investigators stationed at locations where the vast majority of small packages arrive. CPSC will continue to evaluate its staffing model and attempt to identify efficient ways to target and examine potentially unsafe products shipped directly to e-commerce consumers and coordinate better with CBP and ICE.

QUESTIONS SUBMITTED BY HON. MARIA CANTWELL

Question. As the GAO report identifies, CBP does not proactively communicate with online marketplaces that have teams that work closely with the intellectual property rights center, brands, and law enforcement to keep counterfeit items off their sites. However, information sharing is critical.

What are the specific legal parameters for sharing information with e-commerce websites about counterfeit goods CBP seizes?

CBP is currently reviewing options for sharing additional information with rights holders and e-commerce websites. What is the timetable for this review?

What are the differences between the information sharing rules for the CBP and ICE?

How is the relationship with the Intellectual Property Center working? In your view, is CBP getting sufficient information to properly do the job?

Answer. The questions above are focused on CBP's legal authorities and relationship with ICE. Therefore, CPSC has no response on this subject.

Question. CBP and ICE coordinate with several other Federal agencies in their efforts to interdict the flow of counterfeit goods into the United States. As a part of this effort, CBP and ICE also work with rights holders to ensure that their trademarks and copyrights are recorded in the CBP online system. Also, CBP puts a priority on enforcing IP registered with the U.S. Patent and Trademark Office and the U.S. Copyright Office.

According to the GAO report, increasing the number of patents, trademarks, and copyrights with the CBP was an important way that a rights holders can help CBP's enforcement efforts.

Given the benefits of registering patents, trademarks, and copyrights with CBP, does the U.S. Patent and Trademark Office or the U.S. Copyright Office share information with the CBP?

If so, what steps could be taken to improve the sharing of registrant information for new patents, trademarks, and copyrights?

Could the U.S. Patent and Trademark Office or the U.S. Copyright Office forms be adapted to provide simultaneous registration with the CBP?

Answer. The questions above are focused on CBP's interaction with the U.S. Patent and Trademark Office and the U.S. Copyright Office. Therefore, CPSC has no response on this subject.

Question. The U.S. Consumer Product Safety Commission (CPSC) plays an important role in protecting consumers from health and safety hazards. Additionally, CPSC created their import surveillance program 10 years ago. Under this program you combine targeting systems, staffing, and coordination with the CBP and ICE to identify non-compliant and hazardous products.

How often do unsafe, non-compliant, or hazardous seized goods also have intellectual property rights (IPR) violations?

Answer. CPSC does not have data on the number of seized shipments that were both counterfeit and in violation of a CPSC requirement. However, CBP and CPSC have collaborated on a number of shipments where a potential IPR violation and a safety violation were found. Examples include: holiday lights, cell phone wall chargers, lithium-ion batteries used in hoverboards, laptops, and cell phones, children's backpacks, and numerous toys.

A recent example of our successful collaboration with CBP in the area of intellectual property rights enforcement is illustrated by a shipment of counterfeit toys seized by CBP in January 2018 at the Port of Los Angeles. The Commercial Targeting and Analysis Center (CTAC) identified a high-risk shipment from China, imported by a manufacturer that previously attempted to import noncompliant products. CTAC flagged the shipment, which was then examined by CBP and CPSC, and it was found to contain toys bearing counterfeit trademarks of popular children's toys. CPSC determined that the products also contained excessive lead and small parts, in violation of CPSC regulations and the Federal Hazardous Substances Act. This coordination between our agencies resulted in confiscating nearly 2,800 unsafe and fraudulent toys at the port, keeping them from reaching America's children.

Question. Does the CPSC have the resources needed to help combat the IPR problem?

Answer. Although CPSC does not have specific authority to enforce IPR, we do serve as a force multiplier to CBP and ICE in this regard and often make interagency referrals. Thus, additional resources would benefit both CPSC and DHS. Two examples would be co-locating additional CPSC investigators at ports of entry, especially express courier hubs where large quantities of small shipments arrive, as well as continuing improvements and upgrades to CPSC's RAM targeting system.

Question. Do you have sufficient authority to be able to coordinate with other Federal agencies?

Answer. CPSC has sufficient authority to coordinate with our partner agencies. Since passage of the Consumer Product Safety Improvement Act of 2008, CPSC has strengthened its relationship with CBP and closely coordinates with CBP to interdict potentially noncompliant and unsafe imported products. As part of our efforts, CPSC has placed investigators at the largest ports of entry to work side-by-side with CBP staff. CPSC has also stationed staff at the Commercial Targeting and Analysis Center (CTAC) to coordinate with CBP and other government agencies to address import safety issues through commercial targeting.

QUESTION SUBMITTED BY HON. BILL NELSON

Question. What are some examples of counterfeit goods that have caused harm to the health and safety of consumers in recent years?

Answer. Although CPSC's primary focus is targeting products that violate CPSC requirements, we do encounter counterfeit products that also pose a health and safety risk. A recent example of our successful collaboration with CBP in the area of intellectual property rights enforcement is illustrated by a shipment of counterfeit toys seized by CBP in January at the Port of Los Angeles. The Commercial Targeting and Analysis Center (CTAC) identified a high-risk shipment from China, imported by a manufacturer that previously attempted to import noncompliant products. CTAC flagged the shipment, which was then examined by CBP and CPSC, and found to contain toys bearing counterfeit trademarks of popular children's toys. CPSC determined that the products also contained excessive lead and small parts, in violation of CPSC regulations and the Federal Hazardous Substances Act. This coordination between our agencies resulted in confiscating nearly 2,800 unsafe and fraudulent toys at the port, keeping them from reaching America's children.

CPSC and CBP have similarly collaborated on many other shipments where a potential IPR violation and a safety violation were found. Examples include: holiday lights, cell phone chargers, lithium-ion batteries used in hoverboards, laptops, and cellphones, children's backpacks, and numerous toys.

QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL

Question. How many times did CBP Import Specialists encounter fentanyl or fentanyl analogues when inspecting goods for trade violations in 2017? How much fentanyl was seized?

Answer. CPSC does not have jurisdiction over these products and is not involved in the interdiction of fentanyl.

Question. Are Import Specialists trained on safety protocols for encountering dangerous substances like fentanyl?

Answer. CPSC does not have jurisdiction over these products and is not involved in the interdiction of fentanyl.

Question. When an Import Specialist encounters fentanyl, what steps are taken to ensure that other related shipments are searched or flagged for detention before they can enter the United States?

Answer. CPSC does not have jurisdiction over these products and is not involved in the interdiction of fentanyl.

PREPARED STATEMENT OF BRENDA SMITH, EXECUTIVE ASSISTANT COMMISSIONER, OFFICE OF TRADE, CUSTOMS AND BORDER PROTECTION

INTRODUCTION

Chairman Hatch, Ranking Member Wyden, and distinguished members of the committee, thank you for the opportunity to appear today to discuss the enforcement of Intellectual Property Rights (IPR). Trade in counterfeit and pirated goods threatens the health and safety of American consumers, national security, and America's innovation economy. As America's unified border security agency, U.S. Customs and Border Protection (CBP) is responsible for enforcing nearly 500 U.S. trade laws and regulations on behalf of 49 other Federal agencies, and plays a critical role in the Nation's efforts to keep unsafe counterfeit and pirated goods from harming the American public.

In 2016 Congress passed the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA), which expanded CBP's authority to enforce trade laws that affect national security, U.S. business competitiveness, and the collection of revenue—including IPR violations and import safety, two of the seven Priority Trade Issues (PTI) identified by TFTEA—while facilitating lawful international trade.

In fiscal year (FY) 2017, CBP processed $2.39 trillion in imports, 33.2 million entries and more than 28.5 million imported cargo containers at U.S. Ports of Entry (POE). In addition, CBP processes approximately 1.5 trillion in export of goods excluding services. CBP also seized more counterfeit and pirated goods than ever before. Seizures of shipments with violations of IPR increased by 8 percent in FY 2017 over FY 2016. If the seized products had been genuine, the total estimated manufacturer's suggested retail price (MSRP) of the items would have been more than $1.2 billion. CBP's Office of Trade is a critical participant in CBP's multi-layered and multi-faceted approach to identify violations and enforce IPR. Economic benefit modeling shows that the Office of Trade alone provides a $2.1 billion benefit to the American economy through our IPR efforts.

E-COMMERCE

CBP has seen a nearly 50-percent increase in express consignment shipments over the past 5 years. At the end of FY 2017, the average express consignment courier facility in the United States received an estimated 25 million shipments. This same facility received an averaged 2.4 million shipments in 1997, an increase of over 1,000 percent in 20 years. In FY 2013, CBP processed over 76 million express bills and, in FY 2017, CBP processed approximately 110 million bills. In FY 2013, CBP and the U.S. Postal Service (USPS) processed approximately 150 million international mail shipments. By FY 2017, the number of international mail shipments had swelled to over 400 million shipments.

Under TFTEA the *de minimis* value exemption—the value of a shipment imported by one person on one day that generally may be imported free of duties and taxes—increased from $200 to $800. This change has resulted in cost-saving opportunities for importers and consumers that are driving a significant sector of the U.S. economy. Evolving business models, with increasing volumes of imports of small, just-

in-time packages, have significantly altered the dynamic of the international trade environment and CBP's enforcement of IPR and import safety laws. CBP is working with our partners to improve our ability to target illicit shipments in the e-commerce environment while facilitating legitimate trade.

In FY 2017, CBP and ICE–HSI made 34,000 seizures of counterfeit and pirated goods, worth an estimated MSRP of $1.35 billion. Over 90 percent of the seizures were in the express carrier and international mail environments. In FY 2017, during a "small package" blitz at the international mail facility in New York, 43 percent of the packages inspected were non-compliant. During this single event, CBP seized over 5 pounds of fentanyl along with almost 1,300 other non-compliant imports, including 800 counterfeit goods, as well as additional controlled substances. E-commerce shipments pose the same health, safety, and economic security risks as containerized shipments, but the volume is higher and growing. Transnational Criminal Organizations (TCOs) are shipping illicit goods to the United States via small packages due to a perceived lower interdiction risk and less severe consequences if the package is interdicted.

CBP is aggressively working to enhance our enforcement reporting, tracking, strategy, and metrics. For example, in 2016 CBP established the e-commerce and Small Business Branch to manage trade policy and better address various complexities that have emerged as a result from the growth of e-commerce. CBP has been actively engaging with stakeholders, consumers, partner government agencies, and in international forums to better address these challenges in innovative ways. This Branch demonstrates CBP's commitment to support small and microbusinesses while addressing the challenges posed by today's dynamic trading environment.

One of the initial goals of the Branch was to gain a full understanding of the challenges faced at the border related to small shipments. As a result of the Branch's efforts, CBP has finalized an e-commerce strategy that will assist in adapting to a more agile enforcement of e-commerce shipments, create better compliance through new incentives and measures, and educate and engage international trade in order to support the U.S. economy. The strategy will strengthen CBP's ability to protect U.S. consumers, improve managing threats in the e-commerce environment, maximize trade revenue collection, strengthen international mail enforcement, and create stronger, longer-term partnerships here and abroad.

Internationally, the United States is a leader on e-commerce through the World Customs Organization (WCO). In September 2016, the WCO created an e-commerce working group, comprised of customs administrations from WCO member governments, private-sector representatives, international organizations, e-commerce operators/intermediaries and academia, in order to develop solutions supporting needs and expectations of all stakeholders in the e-commerce supply chain. The WCO also created sub-working groups focusing on issues of revenue collection; safety and security; trade facilitation; and data analytics and analysis. CBP co-leads the sub-working group on safety and security.

Finally, in December 2016 and pursuant to title III of the PRO IP Act of 2008, the Office of the Intellectual Property Enforcement Coordinator, within the Executive Office of the President, released a 3-year Joint Strategic Plan for FYs 2017–2019, titled "Supporting Innovation, Creativity and Enterprise: Charting a Path Ahead." CBP is supporting the carryout of the four primary objectives included in the strategy. These objectives are: to enhance national understanding of the economic and social impacts flowing from the misappropriation and unlawful exploitation of intellectual property; to promote a safe and secure Internet by minimizing cyber-enabled, illicit intellectual property-based activities; to secure and facilitate legitimate cross-border trade; and to enhance domestic strategies and global collaboration in support of the effective intellectual property enforcement.

TARGETING AND ENFORCEMENT

In FY 2017, more than 11 million maritime containers arrived at our seaports. At our land borders, another 10 million arrived by truck, and 3 million arrived by rail. An additional quarter billion cargo, postal, and express consignment packages arrived through air travel. Among these are the 110 million express consignment carrier (ECC) shipments and 400 million international mail shipments that arrived in the United States in FY 2017.

CBP uses a multi-layered, risk-based approach to target those shipments deemed to be of highest risk. One of the resources CBP uses in this multi-layered approach is the knowledge and expertise of our regulatory auditors. Strike unit audits begin

when significant or sensitive issues arise, such as increases in health and safety violations, or large volume of counterfeit products are seized. In FY 2017, 16 strike units were assembled and included CBP regulatory auditors, CBP targeting specialists from the National Targeting and Analysis Group (NTAG), and ICE–HSI personnel. CBP and ICE–HSI work closely to complete follow-up enforcement actions resulting from information gathered during these audits.

National IPR Coordination Center

One of the ways TFTEA enhanced IPR enforcement was through the formal establishment of the National Intellectual Property Rights Coordination Center (IPR Center) with joint leadership from ICE and CBP, and permanent CBP staffing. The IPR Center is the lead office within the U.S. Government for coordinating with other Federal agencies on IPR infringement investigations, law enforcement training, and private sector and public outreach.

CBP plays an integral role in the IPR Center, collaborating with ICE–HSI and 23 additional partners at the IPR Center to ensure that border seizures representing criminal activities lead to investigations, arrests and convictions. CBP holds one of the three deputy director positions on the management team at the IPR Center, and is the leading source of referrals to ICE–HSI for criminal investigations. Additionally, staff from CBP's IPR Division (IPRD) attend the weekly Director's staff meeting and all other relevant meetings at the IPR Center. IPRD also coordinates with the IPR Center and the National Cyber-Forensics and Training Alliance (NCFTA) by providing IPR monthly seizure data for de-confliction purposes and potential IPR leads.

The IPR Center has been a key facilitator of INTERPOL's Operation Pangea, an international effort to shut down online pharmacy websites used to sell counterfeit medicine and illicit medical devices. During the most recent operation, Operation Pangea X (September 12–19, 2017), CBP, in coordination with ICE–HSI and the U.S. Food and Drug Administration, effected 1,294 seizures of counterfeit medical devices and illicit medicines. Overall, the operation resulted in the launch of 1,058 investigations, 3,584 websites taken offline, 400 arrests worldwide and the seizure of more than $51 million worth of potentially dangerous medicines.

Trade in illegitimate goods is associated with smuggling and other criminal activities, and often funds criminal enterprises. With the help of CBP and other partners in FY 2016, ICE–HSI arrested 451 individuals, obtained 304 indictments, and received 272 convictions related to intellectual property crimes.

The Commercial Targeting and Analysis Center (CTAC)

Originally established in 2010 as the Import Safety CTAC in support of the July 18, 2007, Executive Order 13439: Establishing An Interagency Working Group on Import Safety, the Commercial Targeting and Analysis Center (CTAC) is a 12-member multi-agency, national trade enforcement coordination center. The CTAC combines the resources and intelligence capabilities of CBP and other government agencies to advance interagency information-sharing and operational collaboration in better protecting the American public from harm caused by unsafe imported products.

The CTAC, led by CBP, is the primary coordination center for operational implementation of title II of TFTEA, titled "Import Health and Safety," including execution of the Joint Importation Safety Rapid Response Plan (JISRRP). The JISRRP is currently within the review and clearance process, but the goal of the JISRRP is to leverage member tools, mechanisms and authorities to identify import safety threats and communicate exigent threat awareness, as well as prescribe mitigating response and recovery actions to agency field operations. Once published, the JISRRP will also provide CTAC members an opportunity to identify and close any current gaps in the joint efforts to address the growing threat of unsafe products imported into the United States.

CTAC's joint targeting and enforcement efforts initiated 243 seizures of unsafe imported products in FY 2017 with an appraised MSRP of more than $3.8 million. Whether it be for counterfeit automotive parts (such as grills, bumpers and brake lines), counterfeit home products, or counterfeit toys—CTAC's rigorous repeat targeting campaigns have resulted in the successful interception of serious threats to consumer safety.

For example, every year in the run-up to the holiday season, CBP seizes thousands of shipments of decorative holiday string lights that have the potential to cause fires or electric shock. These dangerous products are identified through a

CTAC nationwide targeting operation and in close partnership with the U.S. Consumer Product Safety Commission (CPSC).

On January 28, 2018, in another recent example of CTAC joint targeting, CBP officers at the Port of Los Angeles seized a large incoming shipment of toy building blocks for trademark infringement. These counterfeit toys were also found to violate the Federal Hazardous Substance Act for excessive lead and small parts. The shipment was identified through the efforts of CBP and CPSC to target shipments of high-risk consumer products for possible import safety violations.

CBP also established an Interagency Collaboration Division within the Office of Trade. Our Import Safety Division has been closely collaborating and coordinating across Federal agencies to streamline the import process by reducing the redundancy of inspection activities, targeting high-risk trade, ensuring compliance with U.S. trade laws among agencies with overlapping authorities, and deploying risk-based management strategies.

National Targeting Center (NTC)

At CBP's National Targeting Center (NTC), advance data and access to law enforcement and intelligence records converge to facilitate the targeting of travelers and items of cargo that pose the highest risk to our security in all modes of inbound transportation. The NTC processes large amounts of data and uses sophisticated targeting tools and subject matter expertise to analyze, assess, and segment risk at every stage in the cargo/shipment and travel life cycles. As the focal point of that strategy, the NTC leverages classified, law enforcement, commercial, and open-source information in unique, proactive ways to identify high-risk travelers and shipments at the earliest possible point prior to arrival in the United States.

The NTC also works to detect anomalies, trends, and violations in the global supply chain to target high-risk shipments. This high-level analysis helps CBP identify emerging threats, including those posed by TCOs, and to take action to counter these threats. The NTC-Cargo is also leading efforts to de-conflict and coordinate IPR targeting throughout CBP, as well as to ensure timely targeting support for ICE-HSI investigations. There are currently two full-time ICE-HSI Special Agents and two United States Postal Inspection Service (USPIS) employees embedded within the NTC, who serve as liaisons between the NTC and ICE-HSI and USPIS personnel in both domestic and international posts. The NTC also collaborates daily with critical partners from the Drug Enforcement Agency, the Federal Bureau of Investigation, the Food and Drug Administration Office of Criminal Investigations (FDA/OCI), and other members of the Intelligence Community. CBP is sharing information with these agencies and conducting joint enforcement initiatives.

For example, in a single week in June of 2017 approximately 115 seizures where made of counterfeit products by CBP in Puerto Rico, valued at more than $6.5 million. All of these products were illegally imported into Puerto Rico via international mail. This was a record value of counterfeits seized by CBP in Puerto Rico during a single week. A wide range of counterfeited products were seized during the week-long enforcement effort, called Operation Silver Snake, to include pharmaceuticals, electronics, jewelry, apparel, and footwear.[1]

Integrated Trade Targeting Network (ITTN)

Components of CBP's Integrated Trade Targeting Network (ITTN) conducted 12 national-level IPR-mitigating trade operations in FY 2017. The ITTN coordinates all national targeting assets of CBP, including the Centers of Excellence and Expertise, the Tactical Trade Targeting Unit (T3U), CTAC, and the National Targeting and Analysis Groups (NTAGs).

These operations targeted high-risk shipments at seaports, airports, international mail facilities, and express carrier hubs across the United States and resulted in 1,845 seizures of IPR-infringing goods that, if genuine, would have had an estimated MSRP of $44 million. Eight of these operations were conducted by Mobile Intellectual Property Enforcement Teams (MIPETs), teams of CBP IPR experts deployed to assist enforcement operations. MIPET operations in FY 2017 resulted in 1,687 seizures of IPR-infringing goods valued at $34.6 million MSRP and 67 voluntary abandonments.

Centers of Excellence and Expertise

CBP's 10 Centers of Excellence and Expertise (Centers) focus CBP's trade expertise on industry-specific issues through account-based processing on a national scale.

[1] *https://www.cbp.gov/newsroom/local-media-release/cbp-san-juan-stops-millions-counterfeits.*

The Centers, managed from strategic locations around the country, have national authority to make trade determinations at all POEs in an effort to meet the goals of strengthening America's economic competitiveness, enhancing industry knowledge and expertise, developing innovative trade processing procedure, applying strategic and impactful trade enforcement actions, and leveraging available trade intelligence. The Centers serve as resources to the broader trade community and to CBP's U.S. Government partners. By redirecting work to the centralized, industry-specific Centers, the POEs are able to more effectively focus their resources on high-risk shipments and importers that may pose a danger to border security, harm the health and safety of consumers, or violate U.S. trade laws and IPR.

COLLABORATION WITH OUR PARTNERS

TFTEA empowered CBP to collaborate with our partners in new ways, and CBP remains committed to enforcing IPR in accordance to the mandates of TFTEA and in close collaboration with our partners across government and the private sector to ensure that IPR are enforced while facilitating legitimate trade.

TFTEA created the Commercial Customs Operations Advisory Committee (COAC) to advise the Secretaries of the Treasury and DHS on all matters involving the commercial operations of CBP, including advising on significant proposed changes to regulations, policies, or practices. The IPR working group, which falls under the Trade Enforcement and Revenue Collection COAC Subcommittee, is made up of CBP's Federal partners and 19 representatives from multiple industries including express carriers, Customs brokers, and marketplace providers. The group has identified a series of challenges for the consumer, the trade community, and government. One of the main challenges identified was the need for better data collection, automation, and a legal framework for sharing data. The working group also identified education and outreach as a need. As new e-commerce participants may not know they are importers, or understand the responsibilities of being an importer, a mechanism is needed to educate the public. As a follow-up to recent meetings, the working group developed recommendations that CBP is working to implement. The recommendations focused primarily on challenges on section 321/*de minimis* filings. Topics mentioned included data sharing, Partner Government Agency coordination and clarification, and the adoption of policies that would encourage section 321/*de minimis* filings without impeding the flow of commerce.

CBP continues to assess and improve its ability to enforce the laws governing trade in products that are protected by U.S. trademarks and copyrights, and exclusion orders issued by the United States International Trade Commission (ITC). TFTEA provided CBP with new authority to disclose information to the owners of recorded trademarks and copyrights and to persons injured by Digital Millennium Copyright Act (DMCA) violations. CBP concentrates its IPR border enforcement on federally registered trademarks and copyrights that have been "recorded" with CBP by their owners using the Intellectual Property Rights e-Recordation (IPRR) system. CBP administers these "recordations" using a secure proprietary database that CBP can access to make IPR border enforcement determinations. Product ID manuals that are prepared by right holders are also linked to the database and used by CBP in making IPR border enforcement determinations.

Additionally, CBP is able to access information contained in the USPTO trademark registration database.

If CBP suspects that imported merchandise bears a counterfeit mark; constitutes a piratical copy; or violates the DMCA, and CBP determines that the right owner's assistance would help CBP in its ongoing IPR enforcement efforts, CBP is authorized by TFTEA to disclose information appearing on the imported merchandise and its packing or labels to the right owner. IPR owners also assist CBP in identifying authentic and low-risk shipments. As of January 31, 2018, CBP was enforcing 18,302 active recordations, of which 4,477 were copyrights and 13,725 were trademarks.

For example, on March 14, 2017, at Charleston seaport, CBP seized an estimated $1.1 million in counterfeit mobile phone accessories, including phone cases, chargers, cables, and headphones. The merchandise arrived into the port from China and was destined for upstate South Carolina. Examination and appraisal revealed 85,000 individual accessories bearing images and markings from Apple, USB, Bluetooth, Blu-Ray, LG, Marvel, DC Comics, Hello Kitty, and Dr. Dre. CBP reached out to representatives from these companies, who confirmed their images and markings were being used without their permission, enabling CBP to seize these counterfeit goods. Approximately 38,000 power adapters seized bore the Federal Commu-

nications Commission (FCC) mark, signifying they had been tested in an accredited FCC laboratory and met certain operating standards. These were found to be unauthorized markings, a potentially significant safety risk to consumers.[2]

To expand private-sector collaboration and enable CBP to more quickly determine the authenticity of suspected counterfeit goods, CBP published a final rule to allow donations of certain equipment, training, and other support services from the private sector for enforcing IPR. The Donations Acceptance Program, created by section 308(d) of TFTEA, enables CBP to collaboratively explore and implement solutions to trade and travel facilitation and enforcement challenges. On February 15, 2018, CBP announced a new formal partnership arrangement with Procter and Gamble (P&G), as part of the Donations Acceptance Program, to prevent counterfeit P&G products from entering the United States. As the first formal partnership under the Donations Acceptance Program for IPR enforcement, P&G will donate testing devices to verify the authenticity of various P&G products. The devices will help CBP officers and trade specialists quickly determine the legitimacy of the product, reducing the possibility of counterfeit goods entering the U.S. stream of commerce.

CBP will continue to collaborate with private industry through the COAC E-Commerce Working Group. The working group will focus on identifying operational best practices and challenges presented by changing business models and supply chains; the increased volume of e-commerce packages; new complexities presented by e-commerce for businesses of various sizes and industry-type; and evolving compliance and enforcement issues. The group is further identifying workable solutions to e-commerce challenges to create a streamlined path forward for CBP, business, consumers, and the public.

PUBLIC OUTREACH

TFTEA also called for the development and execution of an educational awareness campaign to inform international travelers of the legal, economic, and public health and safety effects of importing IPR-infringing merchandise. During the months of June and July of 2017, as well as November and December of 2017, CBP ran a public awareness campaign entitled "Fake Goods, Real Dangers: The Truth Behind Counterfeits" in eleven airports around the country.[3] All information from the campaign is also prominently displayed on the CBP website as part of CBP's ongoing efforts to keep the public informed about the health and safety dangers to consumers presented by counterfeit and pirated goods. CBP has also revised Form 6059B, the Customs Declaration Form completed by passengers entering the United States, to include a warning to international travelers of the penalties associated with transporting IPR-infringing goods.

CBP constantly seeks to refine and update its outreach to rights owners. To this end, CBP recently prepared a tri-fold brochure titled "How CBP Can Protect Your Intellectual Property Rights," a publication that is geared especially to rights owners who are unfamiliar with what the agency can do to enforce their IPR. The brochure provides a quick snapshot of the enforcement process, calls the reader's attention to the relevant CBP regulations, provides links to more detailed border enforcement guidance available via the *cbp.gov* website, and stresses that IPR border enforcement is a shared responsibility. The brochure then highlights opportunities for right owners to engage CBP and the National IPR Coordination Center. CBP looks forward to making the brochure available at outreach events such as the East and West Coast Trade Symposiums.

CONCLUSION

CBP continues to look to the future of IPR enforcement. Our well-established training program includes rights-holder-conducted webinars, port trainings, and roundtables. In FY 2017, CBP facilitated 18 instructor-led IPR training sessions where over 227 CBP Officers, Import Specialists, and other trade specialists were trained in IPR enforcement. As a result of the hard work of the dedicated men and women of CBP and our partnerships across government and private industry, the

[2] *https://www.cbp.gov/newsroom/local-media-release/charleston-cbp-seizes-11-million-cell-phone-accessories.*

[3] These airports were Baltimore, Washington International Airport, Dulles International Airport, John F. Kennedy International Airport, Dallas/Fort Worth International Airport, O'Hare International Airport, Los Angeles International Airport, Miami International Airport, Atlanta Hartsfield Airport, Newark International Airport, George Bush Intercontinental Airport, and San Francisco International Airport.

combined total number of all IPR border enforcement actions in FY 2017 increased 8 percent over FY 2016.

With the support of Congress, CBP remains committed to protecting businesses and consumers every day through an aggressive IPR enforcement program. We will continue to work in collaboration with our public and private stakeholders and partners to better understand emerging challenges, and to better enforce IPR to protect the health and safety of American consumers and our economy, while facilitating legitimate trade.

Chairman Hatch, Ranking Member Wyden, and distinguished members of the committee, thank you again for the opportunity to testify today. I look forward to your questions.

QUESTIONS SUBMITTED FOR THE RECORD TO BRENDA SMITH

QUESTIONS SUBMITTED BY HON. ORRIN G. HATCH

Question. Given the volume of goods entering the country, what steps do you take to identify and interdict counterfeits?

Answer. U.S. Customs and Border Protection (CBP) employs a layered, risk-based approach to identify and interdict counterfeit goods and other goods imported contrary to U.S. law. The extensive training and technical expertise of CBP Officers, Import Specialists, and other trade professionals are our most reliable assets in interdicting intellectual property rights (IPR) infringing goods. The National Targeting Center (NTC) and the National Intellectual Property Rights Coordination Center (IPR Center) have dedicated staff with national oversight for targeting shipments and for providing field personnel intelligence on suspect shipments entering the United States. CBP also collaborates with U.S. Immigration and Customs Enforcement, Homeland Security Investigations (ICE/HSI) to deter and disrupt the efforts of individuals and organizations whose aim is to exploit U.S. trade and consumers.

CBP works with private industry, 47 partner government agencies, and foreign customs counterparts and other foreign government agencies, to identify trends, anomalies, and high-risk shipments. Foreign customs agencies share information on relevant enforcement actions which can be used for risk assessment.

CBP has many tools at its disposal to identify and interdict shipments of counterfeit goods. Shipment data is transmitted to CBP before cargo arrives in the U.S., and it is used for assessing overall trade compliance and targeting for smuggling and counterfeiting. High-risk shipments are identified for examination via both non-intrusive and physical inspection methods. During examinations, CBP personnel work collaboratively with CBP industry experts, and in some cases consult with the rights holder, to determine whether suspect shipments are counterfeit or legitimate goods. The Centers of Excellence and Expertise are working with CBP headquarters personnel to provide round tables where right holders and CBP personnel can share information and develop best practices on IPR enforcement. CBP also works with the private sector to provide webinars, product identification guides, and in-person training to CBP personnel.

Question. Can you please describe the specific reasons why e-commerce platform data located on the package or within it on an invoice is not being shared with rights holders?

Answer. Section 302 of the Trade Facilitation and Trade Enforcement Act (TFTEA), codified at 19 U.S.C. § 1628a, authorizes CBP, when merchandise is detained, to disclose to rights holders information that appears on merchandise and its packaging and labels. The definition of "packaging," for Customs purposes, means materials and containers in which merchandise is packaged for retail sale. See, *e.g.,* 19 CFR part 181, appendix, part 1, section 2. Thus, CBP may disclose e-commerce platform data, but only if the data appears on retail packaging. Pursuant to CBP's regulations, at 19 CFR part 133.21, CBP may disclose additional information to a right holder following seizure of merchandise bearing a counterfeit mark, including (1) the date of importation; (2) the port of entry; (3) the description of the merchandise from the notice of seizure; (4) the quantity as set forth in the notice of seizure; (5) the country of origin of the merchandise; (6) the name and address of the manufacturer; (7) the name and address of the exporter; and (8) the name and address of the importer.

In Executive Order 13785 ("Establishing Enhanced Collection and Enforcement of Antidumping and Countervailing Duties and Violations of Trade and Customs Laws"), the President included—in section 4(b)—the following direction to the Secretaries of the Treasury and Homeland Security:

> To ensure the timely and efficient enforcement of laws protecting Intellectual Property Rights (IPR) holders from the importation of counterfeit goods, the Secretary of the Treasury and the Secretary of Homeland Security shall take all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders: (i) any information necessary to determine whether there has been an IPR infringement or violation; and (ii) any information regarding merchandise voluntarily abandoned, as defined in section 127.12 of title 19, Code of Federal Regulations, before seizure, if the Commissioner of CBP reasonably believes that the successful importation of the merchandise would have violated United States trade laws.

As discussed elsewhere, in accordance with the President's direction, DHS has been taking "all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders" the two categories of information that the President specified in Executive Order 13785. This has included an ongoing evaluation of the extent to which CBP's disclosure of additional information to rights holders would involve any information that is of the type that is generally covered by the Trade Secrets Act (18 U.S.C. § 1905) and, with respect to any such information, whether Congress—in section 302 of TFTEA, 19 U.S.C. § 1628a, or otherwise—has granted CBP sufficient authority to disclose such information to rights holders. In this regard, section 302 authorizes CBP to provide to a rights holder, for the purpose specified in section 302, "information that appears on the merchandise and its packaging and labels, including unredacted images of the merchandise and its packaging and labels" as well as "unredacted samples of the merchandise" (subject to any applicable bonding requirements). CBP has determined that information located on an invoice located on or within a package is protected by the Trade Secrets Act and that TFTEA section 302 does not provide sufficient authority for CBP to disclose that information to rights holders. This analysis is based on the longstanding definition of "packing" in the Customs valuation laws and international agreements. Specifically, the term "*packaging* materials and containers" is defined for Customs purposes in numerous provisions of CBP Regulations as meaning the "materials and containers in which a good is packaged for retail sale" (emphasis added). However, the term "*packing* materials and containers" is defined as "materials and containers that are used to protect a good during transportation, but [do] not include packaging materials and containers" (emphasis added). CBP regulations matching this meaning for "packing" also comport with the United States–Korea Free Trade Agreement, the United States–Panama Trade Promotion Agreement, and the United States–Columbia Trade Promotion Agreement, all of which explicitly do not include the materials and containers in which merchandise is packaged for retail sale. We glean nothing in TFTEA or its legislative history to suggest disregarding the differentiation between "packaging" and "packing" consistently made in existing statutes and trade agreements. Consequentially, section 302 of TFTEA does not provide CBP with the authority to disclose to the right holders e-commerce platform data located on the package or within the package on an invoice. [Note: As discussed below, CBP has drafted a Notice of Proposed Rulemaking (NPRM) to implement sections 302 and 303 of TFTEA with respect to the seizure of circumvention devices and other copyright-infringing goods. The draft NPRM is currently within the interdepartmental review process.]

However, CBP has statutory authority beyond section 302 of TFTEA, including that provided by 15 U.S.C. § 1124 and 19 U.S.C. §§ 1526 and 1595a, that may provide authority for CBP to promulgate regulations to share e-commerce platform data located on the package or within it on an invoice with rights holders.

CBP has drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process.

Question. The Voluntary Abandonment Program recently concluded the pilot phase. We have heard from several stakeholders expressing concerns about the lack of information sharing in an otherwise relatively cost-effective program. Can you please describe that program and explain why you have been unable to share information with the rights owners or platforms?

Answer. The IPR Voluntary Abandonment Pilot was developed in partnership with the private sector and was supported through a May 22, 2014 formal recommendation by the Commercial Customs Operations Advisory Committee (COAC). The primary goal of the program was to explore alternative methods to seizure for small packages containing IPR-infringing goods in the express environment in an effort to develop processing efficiencies.

On November 1, 2014, CBP initiated the IPR Voluntary Abandonment Pilot at the UPS Express Consignment Facility (ECCF) in Louisville, KY. The IPR Voluntary Abandonment Pilot consisted of an expedited enforcement process whereby the participating carriers worked with CBP to notify the consignee that the shipment contained goods suspected to be counterfeit and offer the consignee an opportunity to cede interest in the merchandise through the execution of an abandonment form. The program grew to include the following locations: DHL ECCF in Cincinnati, OH; the DHL ECCF in Los Angeles, CA; DHL ECCF in Miami, FL; and DHL ECCF New York, NY.

More than 12,000 shipments were abandoned through the IPR Voluntary Abandonment Pilot, representing a significant cost savings to CBP and the removal from commerce of a significant volume of suspected counterfeit goods. Additionally, through the efforts of the participating ports, CBP gained a significant amount of knowledge and experience, which will inform and enhance future IPR enforcement and efficiency efforts. In this regard, the IPR Voluntary Abandonment Pilot presented alternatives that could increase the efficiency of counterfeit interdictions, reduce the amount of resources dedicated to administrative actions, and create overall cost savings for CBP. As this program was instituted as a pilot, the decision was made that current efforts must shift from operating in a pilot status to focusing on addressing operational challenges identified during the pilot phase, developing the necessary legal framework to support IPR abandonment procedures, and specifically creating regulations that will allow CBP to share information with right holders when a suspected IPR shipment is abandoned.

In February 2018, formal guidance was issued to impacted CBP ports that the IPR Voluntary Abandonment Pilot was ending. Based on lessons learned from the pilot, CBP has issued additional guidance to field on the use of alternatives to seizures for IPR enforcement purposes. Additionally, as mentioned above, CBP is developing regulatory changes that will allow CBP to share information with right holders when a suspected IPR shipment is abandoned.

Question. Do you believe that § 302 of the Trade Facilitation and Trade Enforcement Act (TFTEA) provides you broad authority to share information with rights holders and trademark owners?

Answer. Section 302 of TFTEA provides CBP with authority to disclose, at detention, in cases of merchandise suspected of (1) bearing a counterfeit mark, (2) constituting a piratical copy of a protected work and/or (3) circumventing a technological protection measure in violation of the Digital Millennium Copyright Act (DMCA), information that appears on imported merchandise, its retail packaging and labels. As such, section 302 provides additional statutory authority for the disclosure regime that CBP has previously promulgated by regulation in respect of suspected counterfeit marks, and extends it to matters involving suspected copyright and DMCA violations.

CBP appreciates the broader statutory authority to disclose information that otherwise might be protected by the Trade Secrets Act (18 U.S.C. § 1905).

Question. If so, does that breadth also allow you the ability to share information before a seizure has been effectuated? If not, please provide counter-citations to other applicable statute or regulations that preclude you from being able to share that information.

Answer. As discussed elsewhere, DHS has been taking "all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders" the two categories of information that the President specified in Executive Order 13785. This has included an ongoing evaluation of the extent to which CBP's disclosure of additional information to rights holders would involve any information that is of the type that is generally covered by the Trade Secrets Act (TSA), 18 U.S.C. § 1905, and, with respect to any such information, whether Congress—in section 302 of TFTEA, 19 U.S.C. § 1628a, or otherwise—has granted CBP sufficient authority to disclose such information to rights holders.

The Trade Secrets Act bars the unauthorized disclosure by government employees of any confidential business information received in the course of their employment. Case law interpreting the statute, which includes Supreme Court decisions and the Act's legislative history, demonstrates that it covers most commercial or financial data collected by any Federal employee from any source.

While section 302 of TFTEA provides for the disclosure of certain information, *i.e.,* information that "appears on the merchandise and its packaging and labels," at detention, *i.e.,* pre-seizure or pre-abandonment, section 302 does not provide sufficient authority to disclose information appearing on packing, which CBP defines as "all containers, exclusive of instruments of international traffic, and coverings of whatever nature, used in placing the merchandise packed ready for shipment to the United States" (19 CFR § 152.102(e)). Moreover, the phrase "appears on the merchandise and its packaging" further limits the disclosure. For example, it does not include the disclosure of information that is contained on or within the packing, *e.g.,* a "fulfilled by Amazon" (FBA) number, or an invoice or packing slip enclosed with the packing. Such information would be considered packing as opposed to packaging, and that distinction is salient in CBP regulations reflecting U.S. trade agreements. Specifically, the term "*packaging* materials and containers" is defined for Customs purposes in numerous provisions of CBP Regulations as meaning the "materials and containers in which a good is packaged for retail sale" (19 CFR part 181, appendix, part I, section II (the NAFTA Rules of Origin Regulations), emphasis added). However, the term "*packing* materials and containers" are defined as "materials and containers that are used to protect a good during transportation, but [do] not include packaging materials and containers" (*Id.,* emphasis added). CBP regulations matching this meaning for "packing" also comport with the United States–Korea Free Trade Agreement, the United States–Panama Trade Promotion Agreement, and the United States–Columbia Trade Promotion Agreement, all of which explicitly do not include the materials and containers in which merchandise is packaged for retail sale. We glean nothing in TFTEA or its legislative history to suggest disregarding the differentiation between "packaging" and "packing" consistently made in existing statutes and trade agreements. Consequentially, section 302 of TFTEA does not provide CBP with the authority to disclose to the right holders e-commerce platform data located on the package or within the package on an invoice, such as a "fulfilled by Amazon" (FBA) number. [Note: As discussed below, CBP has drafted a Notice of Proposed Rulemaking (NPRM) to implement sections 302 and 303 of TFTEA with respect to the seizure of circumvention devices and other copyright-infringing goods. The draft NPRM is currently within the interdepartmental review process.]

However, as noted above, CBP has statutory authority beyond section 302 of TFTEA, including that provided by 15 U.S.C. § 1124 and 19 U.S.C. §§ 1526 and 1595a, that may provide authority for CBP to promulgate regulations to share e-commerce platform data located on the package or within it on an invoice with rights holders.

CBP has drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process.

Question. Do you agree that § 303 of TFTEA provides CBP with broad authority to seize circumvention devices?

Answer. As it related to circumvention devices, CBP believes that it has authority to enforce the DMCA; however, CBP appreciates the additional clarity that section 303 affords in this regard.

Question. If so, when do you anticipate release regulations to significantly expand enforcement of this provision in the law?

Answer. CBP has drafted a Notice of Proposed Rulemaking (NPRM) to implement sections 302 and 303 of TFTEA. The draft NPRM is currently within the interdepartmental review process.

In addition, as noted in the prior responses to questions 2 and 4, CBP has also drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process.

Question. You have recently mentioned difficulties with passing new regulations in a timely fashion due to required reviews of all regulations by the Department of Treasury. Can you please describe, in detail, the process now in place at CBP for promulgating new regulations?

Answer. Since the enactment of the Homeland Security Act of 2002 and the issuance of Treasury Department Order No. 100–16, CBP is in the position of having some of the regulations it drafts approved by the Department of the Treasury and some regulations approved by the Department of Homeland Security (DHS). Under the Homeland Security Act, Treasury retained its traditional authority over Customs revenue functions. Although Treasury delegated much of its retained authority to CBP, if a regulation involves a Treasury-retained Customs revenue function, the Department of the Treasury has sole authority to approve the regulation. Treasury-retained Customs revenue regulatory topics include certain of the subjects on which implementing regulations are necessary under TFTEA. For example, regulations for which the Department of the Treasury retains authority include those relating to copyright and trademark enforcement and those relating to the completion of entry or substance of entry summary including duty assessment and collection. While the Department of the Treasury has the sole authority to approve these Treasury-retained Customs revenue function regulations, DHS has an interest in reviewing these regulations prepared by CBP, as a component agency, before the regulations are sent to Treasury.

Accordingly, the process at CBP for promulgating new regulations under TFTEA involves CBP drafting a regulation, putting it into CBP component review for all interested offices within CBP to review, comment, and approve, including its Office of Chief Counsel, before the Commissioner signs the document. After the Commissioner signs the document, it is sent to DHS, including its Office of General Counsel, for review and clearance. After DHS clears the regulatory document, the document is sent to the Department of the Treasury for approval. The Department of Treasury, including its Office of General Counsel, reviews the package. The Department of Treasury then interacts with the Office of Management and Budget (OMB) to determine whether OMB needs to review the draft regulation under Executive Order 12866. If OMB does not need to review the Treasury-retained Customs revenue function regulation, the regulation can then be finalized and signed by the Deputy Assistant Secretary of the Treasury and sent to the Federal Register for publication. If OMB determines that OMB review is required (and OMB review generally includes routing the packages through interagency and interdepartmental review), the review will take place and the regulation will be finalized after OMB review has been concluded.

Question. What ways can that process be streamlined while still ensuring competent, effective, and legally sound regulations?

Answer. CBP understands the policy and legal interests that both DHS and Treasury have in Treasury-retained Customs revenue function regulations, and their review helps to ensure the issuance of competent, effective, and legally sound regulations. While there is limited opportunity to streamline this process, all involved parties maintain close coordination, and matters that have been determined by CBP leadership to warrant prioritization are drafted and moved to publication as expeditiously as possible.

Question. TFTEA created the national IPR center to help coordinate the work of more than a dozen agencies for intercepting and enforcing intellectual property rights. Because the program is so new, we are interested in learning what has been effective and what could be improved. What do you think the National IPR Center does well, and what do you think it could improve on?

Answer. The Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA) formally codified the National Intellectual Property Rights Coordination Center (IPR Center), which was administratively established in 2000. The IPR Center is led by ICE/HSI, and CBP provides substantial support for it, by establishing permanent staff at the IPR Center in excess of the number of staff mandated in TFTEA. The IPR Center currently has 23 partner agencies, including four foreign partners. The IPR Center is highly effective at case de-confliction, the deliberative process of presenting all possible investigative leads and intelligence products to all partner agencies in order to bring forth all relevant information. This ensures that agencies are all aware of interest in any particular suspect entity. More importantly, agencies are able to determine if another agency has an open case or strong interest in pursuing a new case. This prevents conflicting investigations that could damage an investigation or even put investigators in jeopardy. It also incentivizes cooperation

and partnerships during investigations and cases that preserve agency resources and maximize positive outcomes. To that end, CBP is working toward better operational coordination and sharing of information about risks and results with partner agencies, particularly ICE/HSI and the FBI, two principal agencies at the IPR Center.

Question. As the FY 2016 GAO seizure statistics noted, CBP processed over 32 million shipments and seized 31,560 shipments of IPR-infringing goods worth an estimated $1.38 billion. As a parallel, the Postal Service, through the substantial growth of its international small parcel business saw significant increases of shipments processed as well. International small parcels within the U.S. Postal Service increased 232 percent from 2013 to 2017, when it received nearly half a billion packages. With so many packages processed through both U.S. Ports of Entry and International Mail Facilities, how does the CBP focus on the targeting of unlawful shippers who traffic in counterfeit goods?

Answer. The targeting of entities for trade enforcement purposes, including shippers who traffic in counterfeit goods, is primarily (outside of certain pilot programs described below) a manual process in mail unlike that of express consignment where automated systems and advance electronic data are employed in the risk assessment. Utilizing risk management principles and techniques, mail parcels are selected for inspection based on criteria that fluctuates with the trends and threats identified by CBP personnel. Various factors and risk indicators are evaluated in the selection of mail parcels for examination. Factors may include physical features of the packaging or textual information such as the description of the goods on the Customs declaration. Examples of risk indicators are the use of a fictitious company name or address as well as the situation where a shipment originates from a country where genuine goods are not made. CBP personnel also utilize internal systems to determine past seizure history and review intelligence in order to enhance the focus of targeting efforts.

Question. If USPS were to provide electronic advance data to CBP, could that be used to target counterfeit goods?

Answer. Based on the preliminary results from an advance electronic data (AED) pilot between CBP and the USPS, there are promising opportunities with AED for enhanced trade enforcement targeting, trade facilitation of low risk shipments, and capability for big data analytics. The AED from the USPS and/or foreign postal agencies could result in improved and effective targeting of counterfeit goods provided the data from all countries is mandatory, timely, abundant, and accurate.

CBP completed a Memorandum of Understanding with the USPS on September 1, 2017 that enhances targeting capabilities. The MOU solidifies the interagency partnership between CBP, USPS and the Inspection Service at all IMFs. The partnership is in place at New York, the largest International Mail Facility (IMF), and has expanded to a total of five IMFs. The current pilots began in 2014 and 2015 and target certain mail for inspection using some of the AED obtained under data-sharing agreements with postal operators. Under the pilots, CBP uses AED to target a small number of pieces of mail each day. Since the pilots began, USPS has made efforts to locate and provide CBP with the targeted mail and CBP has collected performance data on the percentage of targeted mail USPS has provided for inspection. The USPS currently provides CBP with AED from Australia, Canada, China, Hong Kong, France, Germany, S. Korea, Spain, Singapore, and the UK. CBP's AED pilot program with the USPS has proven useful for CBP to make informed targeting and enforcement decisions regarding international mail shipments.

With respect to counterfeit goods, we have demonstrated some success through the use of AED. For example, the CBP Office of Trade, Los Angeles National Threat Analysis Center used AED incorporated into CBP's Automated Targeting System (ATS) for inbound international mail that enabled the successful targeting and seizure of six shipments of counterfeit networking equipment affixed with counterfeit U.S. trademarks. Those six shipments were seized in January through March 2018 at four different CBP IMFs and had a total MSRP value of $674,000. In early 2017, CBP officers successfully targeted and intercepted a shipment of fentanyl. Through further research of the AED, CBP collected additional information that implicated a transnational criminal organization using the "dark web" to distribute the illegal substance. CBP, in collaboration with the United States Postal Inspection Service and other Federal Law Enforcement agencies, was able to develop actionable intelligence that identified additional high-risk targets. This also allowed CBP to affect seizure of subsequent fentanyl shipments in the postal stream.

Question. Would it be feasible to institute a U.S. Postal Service known shipper program so that criminals who ship counterfeits could be identified at an earlier stage?

Answer. CBP defers to the U.S. Postal Service on this question.

QUESTIONS SUBMITTED BY HON. RON WYDEN

Question. In one way or another, you all touched on the shift from containerized shipping to small packages. You have also highlighted the challenges in enforcement against counterfeit goods.

Given that we seem to be in a new era of trade, wouldn't you agree that the Federal Government's enforcement strategy to go after counterfeit goods needs to adapt to the changing market? If so, what changes would you recommend in current CBP and ICE enforcement priorities and approaches?

Answer. Yes. CBP is adjusting its enforcement strategy to address the unique challenges posed by the small package environment. On March 6, 2018, CBP released its E-Commerce Strategy, which details objectives for adapting CBP's enforcement posture to address the challenges associated with the rapid increase in volume in small packages. This includes enhancing legal and regulatory authorities, enhancing CBP operations to respond to emerging supply chain dynamics, driving private sector compliance, and facilitating international trade standards for e-commerce. In conjunction with the E-Commerce Strategy, CBP has planned initiatives to enhance its IPR enforcement posture in the small package environment that includes improving training, developing processing efficiencies, and improving operational coordination and collaboration on policy development. CBP supports efforts to increase shipping data in the international mail environment and will continue to partner with ICE on a daily basis on IPR issues through its permanent staff located at the IPR Center. Additionally, CBP works both bilaterally and through multilateral fora such as the Border Five and the World Customs Organization to set international standards and develop best practices.

Question. Ms. Smith, in the Trade Facilitation and Trade Enforcement Act authored by Senator Hatch and myself, we created new information sharing authorities for CBP to work with rights holders and others to identify and prevent the importation of counterfeit products. And yet, that is an area where GAO, and many U.S. companies, find that CBP is not sharing enough information with e-commerce platforms and other market participants to most effectively combat illegal imports.

You stated at the hearing that CBP does need additional legislative authority to share information more effectively, but that it had not identified what authority is needed. You confirmed that you would seek to meet a 60-day deadline for identifying the authority you need. I encourage you to take a comprehensive view of CBP's information sharing to help trademark holders and platforms participate in identifying the source or manufacturer of counterfeit products.

Will you commit to working with my staff to also identify what information is currently being shared, whether it is being done consistently across ports, and where CBP currently has the authority to share additional information?

Answer. CBP absolutely believes in partnership with you and your staff, and looks forward to working with Senate Finance Committee staff to construct a robust disclosure regime that will further our shared goal of interdicting IPR-violative merchandise at the border while providing rights holders with increased disclosure.

CBP will work with the committee to build upon CBP's ongoing efforts to expand its ability to share information in efficient and consistent manners. These efforts include work conducted as part of the Voluntary Abandonment Pilot that concluded in February 2018 and CBP's work to identify any needs for additional legal authorities for information sharing with the private sector under Executive Order 13785 titled "Establishing Enhanced Collection and Enforcement of Antidumping and Countervailing Duties and Violations of Trade and Customs Laws."

As discussed elsewhere, DHS has been taking "all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders" the two categories of information that the President specified in Executive Order 13785. To this end, CBP has drafted a Notice of Proposed Rulemaking (NPRM) to implement sections 302 and 303 of TFTEA with respect to the seizure of circumvention devices and other copyright-infringing goods. The draft NPRM is

currently within the interdepartmental review process. CBP has also drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process. CBP's initiatives have also included an ongoing evaluation of the extent to which CBP's disclosure of additional information to rights holders would involve any information that is of the type that is generally covered by the Trade Secrets Act (18 U.S.C. § 1905) and, with respect to any such information, whether Congress—in section 302 of TFTEA, 19 U.S.C. § 1628a, or otherwise—has granted CBP sufficient authority to disclose such information to rights holders.

Question. Ms. Smith, year after year, CBP puts out information on the total number of counterfeit goods seized by CBP, but we don't really have a sense of what impact this is having on the number of counterfeit imports coming into the country. What we really need is intelligent effective enforcement that reduces the flow of counterfeits into our country.

Do you agree with me that this means not only targeting and inspecting packages, but also gathering information to go after foreign manufacturers, and individuals in the United States who knowingly import and re-sell counterfeit goods?

Answer. Thank you for recognizing the significant increase in seizures, to over 30,000 in each of the last two fiscal years, which we believe is a result of continuing to improve upon sophisticated targeting and enforcement mechanisms. We are proud of these accomplishments, but we agree that CBP's enforcement in this area needs to be constantly evolving. In a recent study on illicit trade, the OECD estimated that 2.5 percent of global trade involved trade in counterfeit goods. Our strategy is to educate first time importers and online shoppers and consumers who simply do not know the rules, while focusing targeting and enforcement resources on identifying and stopping the bad actors who are deliberately dealing in counterfeit goods and committing a host of other trade-related crimes. CBP desires to gain more information on international mail packages via advanced electronic data. We continue to work with our domestic law enforcement partners and in international forums to identify the most problematic bad actors. CBP continuously works to improve how we use information and advanced targeting to identify the worst violators. CBP utilizes systems such as Automated Targeting System (ATS) to assign risk scores for potentially suspect shipments. Shipments that are targeted for exam and found to be violative are seized and all inspection and seizure information is entered into ATS. CBP is able analyze historical violator data in ATS and link inbound shipment data to these bad actors. CBP is looking at various predictive analysis systems for risk identification to determine, in advance, when violative goods might enter the U.S. This capability would allow CBP to more efficiently target for violations.

CBP also partners with ICE–HSI to enforce both civil and criminal trade laws. CBP staffs the National Intellectual Property Rights Center and works with all of the Federal partners to investigate IPR infringement. In FY 2017, ICE–HSI arrested 457 individuals, obtained 288 indictments, and received 242 convictions related to intellectual property crimes.

Question. Do you commit to making that a priority in CBP's strategy for combating counterfeits and to cooperate with foreign authorities as mandated by section 309 of the Trade Facilitation and Trade Enforcement Act of 2015?

Answer. CBP Attachés or CBP Advisors are posted in over 25 countries. CBP offices will coordinate with in-country CBP Attachés and other CBP Office of International Affairs personnel to work with foreign customs counterparts, both bilaterally and multilaterally, with the goal of attaining more and better data for improving risk assessment, targeting, detection, and interdiction of IPR-infringing products arriving at the U.S. border. Such cooperation may include information and data exchange, coordinated operational work, sharing of best practices and trend analysis, and participating in bilateral and multilateral working groups (including the World Customs Organization Counterfeiting and Piracy Group and the APEC Subcommittee on Customs Procedures (SCCP)). CBP and representatives of partner governments that are posted at the National Intellectual Property Rights Coordination Center (IPR Center) and National Targeting Center work closely with CBP and work together with targeters and intelligence staff to detect violators and to advance anti-counterfeiting policies, programs and operations of mutual interest.

Additionally, the 80 Customs Mutual Assistance Agreements (CMAAs) facilitate the exchange of information, evidence, and other mutual assistance between Customs administrations to prevent, detect, and investigate Customs and other trade law offenses. As legally binding executive-level agreements, CMAAs establish the legal framework and the obligation for the parties to share information with each other. CBP is able to utilize these agreements to work with partner countries to exchange information on Customs-related matters, including exports, imports, and transshipments that may contain counterfeit, grey market, prohibited, or unsafe goods. CBP can make requests for information on such shipments to facilitate its trade enforcement activities. CMAAs also serve as foundational documents for subsequent information sharing, including the sharing of Customs administration best practices, embedding of personnel internationally, training and capacity building, and mutual recognition arrangements on authorized economic operator programs.

Question. Ms. Smith, in your testimony, you stated that CBP has seen a nearly 50-percent increase in express consignment shipping, such as through UPS or FedEx, over the past 5 years, and 1,000 percent in the last 20 years. As I said in my opening statement, I think that is a good thing, and represents an opportunity for small businesses in Oregon and across the country. But, as trade flows are transforming, CBP needs to transform too. To date, that has not happened. In fact, CBP continues to fall behind in the basics, such as hiring enough officers to ensure that all of our trade laws are being enforced.

I understand that CBP has concluded a multi-million dollar contract with a private company to recruit and hire 5,000 Border Patrol Agents and 2,000 CBP Officers in the next 5 years. I am deeply skeptical that we need to assemble a small army of Border Patrol Agents when illegal crossings are at historic lows. Meanwhile the 2,000 hires will likely barely meet the trade enforcement needs of CBP (much less the travel and trade facilitation functions), according to CBP's own "resource optimization model." I am disappointed in the apparent prioritization of Border Patrol Agent hiring. Could you tell me what other efforts you are making to onboard personnel with trade enforcement functions?

Answer. The Consolidated Appropriations Act of 2018 H.R. 244 included an additional $8.9 million dedicated to hiring trade enforcement staffing. The Office of Trade (OT) was authorized to hire 140 TFTEA positions, and we are steadily hiring to fulfill this mandate through recruitment, using various hiring authorities, and participating in hiring events. In fiscal year 2018, OT has completed hiring of 60 persons (25 internal and 35 external candidates) who will support trade enforcement initiatives and programs. We will continue to hire in earnest throughout the rest of the year and use fiscal year 2019 funds, if appropriated.

We have also utilized unique staffing solutions to begin fulfilling the TFTEA mandates:

- To develop new regulations, legal staff and economists had to be assigned from the existing pool of staff to draft new regulations and notices of proposed rulemaking. Additionally, operators, financial analysts, and system developers had to be included in the process to ensure approaches met the expectations of TFTEA, but were also feasible from an operations and automation perspective for OT, OFO, and OF.
- For EAPA, OT stood-up the division via temporary assignments and requests for mutual support from various offices in CBP including OFO, OF and INA. Fully staffing the EAPA division will be a priority going forward with fiscal year 18 funding.
- Standing up TRLED and the Trade Enforcement Task Force to address Forced Labor were accomplished through a realignment of existing staffing into the newly designed directorate, and an aggressive recruiting plan to staff the Task Force through temporary assignments with staff from OT and OFO. The Forced Labor workload still remains, and will shift to permanent hiring for TRLED under TFTEA with FY18 funding.
- Positions specified by TFTEA to support the IPR Center were accomplished with longer term temporary assignments. Permanently staffing these positions will be accomplished using FY18 TFTEA funding.
- Audit staff to support Forced Labor, EAPA, AD/CVD and IPR as a focus of TFTEA was stretched to accommodate immediate operational needs, and fiscal year 18 staffing funding will bring new auditors on-board to help balance this new workload with planned audits.

Question. At the same time that the United States must re-examine enforcement as trade flows change, it must also ensure that U.S. businesses are in position to

reap the benefits of modern commerce. That is why Congress raised the *de minimis* threshold in the Trade Facilitation and Trade Enforcement Act of 2015. And it is why I support the administration's participation in work on electronic commerce issues at the WTO.

What is CBP doing at the World Customs Organization and other fora to ensure that the United States is a leader on cooperation and initiatives around electronic commerce facilitation, as well as enforcement?

Answer. The United States leads at the World Customs Organization (WCO) and in other international forums on the development of best practices and the creation of advisory documents relating to the management of Customs and other trade enforcement. This includes recent work relating to the significant changes to international trade flows brought on by the phenomenon of e-commerce. For example, in 2016, the WCO created an e-commerce working group to develop best-practices in the context to address Customs enforcement of e-commerce shipments and unique challenges these shipments present for overall Customs management (*i.e.,* the movement from large containers with consolidated goods via ocean and land shipping to small individually-entered packages via express consignment and postal mail). Multiple challenges were identified regarding e-commerce shipments, including: ensuring connectivity via Customs (revenue collection, trade facilitation, and risk management), lack of or poor quality information associated with these shipments for risk-assessment and other enforcement efforts, varying authorities, and other legal abilities Customs agencies to develop global standards of Customs treatment, and the entrance of new players to international trade, including growing on-line sales platforms, transaction facilitators, medium to small vendors, and one-time buyers/sellers. In particular, the working group strives to determine best practices for how to incorporate small businesses into Customs administrations' present programs and relationships formed with traditional larger importers/exporters, and how to best ensure these smaller actors are aware of their obligations as importers/exporters under Customs and related trade enforcement laws. The working group currently drafts an e-commerce framework of standards seeking to address the changing trade landscape. This includes heightened security concerns and the needs/challenges of both the private sector and Customs administrations to comprehensively manage. There are multiple topics in the CBP E-Commerce Strategy that complement the framework such as education, and outreach of the public, and private sector. In addition, both documents agree that a known shipper/trusted trader type program should be created to mitigate high risk shipments. The United States continues to work through the interagency process, and with the WCO to improve the framework. The growing and changing risk presented by the phenomenon of e-commerce. The WCO and its member administrations met on April 9th–13th to discuss and edit the document, and will likely be extending the deadline for the framework until spring 2019, given the significant volume of work still to be completed and the establishment of consensus on the approach. The United States was actively engaged in this process, including delegates from CBP and other U.S. Government agencies. The WCO is a legally non-binding organization unlike the World Trade Organization and the best practices established in the non-binding framework will be influential in subsequent establishment of national legislation of Customs administrations'. The United States' engagement in this and all international forums will be consistent with our WTO legal obligations and with the Trade Facilitation and Trade Enforcement Act of 2015.

The United States is also leading efforts with Border Five countries (Australia, New Zealand, Canada, the United Kingdom, and the United States) and at the Asia Pacific Economic Cooperation (APEC). The United States has proposed the development of APEC e-commerce operation. The United States has also met several times with the Border Five on e-commerce, most recently meeting in Seattle, WA. Both groups have shared best practices and case studies. The United States has also shared the CBP E-Commerce Strategy with the WCO, Border Five, and APEC as a best practice on how to manage the increasing challenges of e-commerce low value shipments.

QUESTIONS SUBMITTED BY HON. PAT ROBERTS

Question. The GAO study on how agencies can improve efforts to address risks posed by changing counterfeit markets found growth in e-commerce has attributed to counterfeiters producing a wider variety of goods sold on popular websites alongside authentic goods. The goods are often deceiving to consumers, due to counter-

feiters gaining an appearance of legitimacy on third-party online marketplaces. What tools are readily available to empower consumers to make educated decisions when purchasing from third party sellers on e-commerce platforms?

Answer. In 2017, CBP developed and ran the "Truth Behind Counterfeits" public awareness campaign, targeting travelers in the major airports. The goal of the campaign was to educate travelers and influence their consumer behavior. With messages such as "Fake Goods, Real Dangers," CBP's goal is to empower the public with the knowledge that counterfeit products have harmful and dangerous consequences; therefore, it is important to shop from reputable sources. So far, CBP has conducted two phases of the campaign during the high travel periods of summer 2017 and December 2017. By placing large advertisements in various airports and through digital ads, CBP has reached and estimated 202 million people. CBP is currently implementing the third phase of the campaign, which is running this summer.

In addition, CBP created public awareness "road shows" which are made up of IPR personnel setting up an exhibit of seized items at various airports throughout the country. The road shows provide a more focused and direct way to educate the public about the harms associated with IP infringing goods and ways to determine the validity of products by showing examples of a variety of counterfeit products. CBP personnel provide these individuals with knowledge to protect themselves and their families and alert them to be cognizant about goods they may purchase in person and through online platforms. To date CBP has spoken with approximately 5,000 people through these events.

CBP created a dedicated website for the campaign with more information for the consumer: *https://www.cbp.gov/FakeGoodsRealDangers.*

Additionally, CBP allows the public to report suspected counterfeits through the online E-Allegations portal: *https://eallegations.cbp.gov/Home/Index2.*

Question. The U.S. Customs and Border Protection (CBP) has over 75 Customs Mutual Assistance Agreements (CMAA) with foreign governments allowing for the exchange of information and intelligence that help investigate and prevent Customs offenses. CMAAs are vital in the United States efforts to fight terrorism and other trafficking offenses. How can CBP leverage these agreements to combat counterfeit goods?

Answer. Customs Mutual Assistance Agreements (CMAA) are binding bi-lateral executive-level international agreements, negotiated and enforced by their respective Customs administrations. CMAAs are negotiated by CBP and U.S. Immigration and Customs Enforcement—Homeland Security Investigations (ICE–HSI), and signed on behalf of the United States.

CMAAs provide a legal framework for the exchange of information and evidence to assist countries in enforcement against Customs offenses. CMAAs aid in the prevention, detection, and investigation of crimes associated with goods crossing international borders, counterfeit and other IPR violative items. CMAAs also are used to assist in judicial and quasi-judicial proceedings involving suspected violations of Customs laws, by ensuring evidence and supporting information is usable under chain of evidence standards in the United States and in foreign jurisdictions. CMAAs also serve as foundational documents for subsequent information sharing arrangements for deeper engagement on IPR enforcement, including the sharing of Customs administration best practices, embedding of personnel internationally, training and capacity building, and mutual recognition arrangements on authorized economic operator programs (pre-vetted exporter/importers, freight forwarders, and Customs brokers). CMAAs are also excellent means of establishing greater bilateral cooperation by law enforcement officials. CMAAs work to facilitate trade by enabling greater information flows in regard to searches, seizures, detentions, audits, and other enforcement actions, allowing trade to flow more freely.

QUESTIONS SUBMITTED BY HON. JOHN THUNE

CBP AUTHORITY TO SHARE INFORMATION ON COUNTERFEITS

Question. The Trade Facilitation and Trade Enforcement Act requires CBP to consult with the private sector on areas for collaboration and training.

What can CBP do to accelerate the agency's efforts to engage with the private sector and meet full commitments to TFTEA implementation to reduce further the

amount of counterfeit products that end up in our domestic economy and potentially threaten the safety of American consumers?

Answer. CBP has made significant progress in meeting TFTEA requirements related to private-sector engagement, collaboration, and training. Continued collaboration in these IPR initiatives and training will build upon CBP's success.

Section 308(d) of the Trade Facilitation and Trade Enforcement Act of 2015 (Pub. L. 114–125) mandates that the Commissioner prescribe regulations enabling CBP to receive donations of hardware, software, equipment, and technologies for Intellectual Property Rights (IPR) enforcement purposes, 19 CFR § 133.61—Donations of Intellectual Property Rights Technology and Support Services, was published on December 15, 2017, and became effective on January 16, 2018. To support this requirement, the Intellectual Property Rights Donation Acceptance Program (IPR DAP) was developed with the intent of establishing partnerships with private sector donors to provide IPR testing equipment and technologies that can be used at the ports of entry, labs or otherwise to support IPR enforcement.

The IPR DAP is a mechanism for government and industry partnership and is a way to develop mutually beneficial programmatic and operational improvements for IPR enforcement. On February 15, 2018, CBP entered into first formal partnership under the IPR Enforcement Donation Program with Procter and Gamble (P&G). P&G donated, and will resupply as needed, testing devices and kits to help CBP officers and trade specialists quickly determine the legitimacy of various P&G products, reducing the possibility of counterfeit goods from entering the U.S. stream of commerce.

The IPR DAP is a mechanism by which to collaboratively explore and implement tangible solutions to trade and travel facilitation and enforcement challenges. The opportunities for collaboration under this program are very exciting and CBP encourages interested parties to consider participation in the program.

Section 308 of TFTEA mandates that CBP provide IPR-specific training and consult with the private sector on the use of new technologies for IPR enforcement. CBP has a well-established training program, which includes right holder conducted webinars, port trainings, and industry specific roundtables. In fiscal year 2016, CBP facilitated 36 instructor-led IPR training sessions where over 600 CBP Officers, Imports Specialists, and other trade specialists were trained in IPR enforcement. So far, in fiscal year 2018, CBP has conducted four instructor-led IPR training sessions and nine right holder hosted webinars. CBP will continue to expand right holder webinar trainings. Additionally, CBP is in the early stages of developing an advanced IPR training course with the goal of incorporating hands-on, right holder training, in a live or simulated environment.

Question. Ms. Smith, the GAO's second recommendation called on CBP to share information with the private sector, either through new regulations or requesting additional authority from Congress if necessary.

What is CBP's view as to whether the agency has sufficient regulatory authority to share information on seized counterfeits with e-commerce companies, both the direct vendor and the Internet platform companies through which so many e-commerce transactions occur? In particular, I'd like to understand CBP's position on sharing information on seized shipments of counterfeits with Internet platform companies—like EBay or Amazon—since these companies seem to be well positioned, and I believe willing, to help anti-counterfeit efforts as well as assist in public safety efforts when counterfeit goods pose such threats. Please help us understand the scope of authority CBP needs to share information with appropriate third parties when counterfeit goods are identified and seized?

Answer. As discussed elsewhere, DHS has been taking "all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders" the two categories of information that the President specified in Executive Order 13785. This has included an ongoing evaluation of the extent to which CBP's disclosure of additional information to rights holders would involve any information that is of the type that is generally covered by the Trade Secrets Act (18 U.S.C. § 1905) and, with respect to any such information, whether Congress—in section 302 of TFTEA, 19 U.S.C. § 1628a, or otherwise—has granted CBP sufficient authority to disclose such information to rights holders.

While section 302 of TFTEA provides for the disclosure of certain information to rights holders, CBP has determined that it does not authorize CBP to disclose information to third parties such as e-commerce platform owners. However, once infor-

mation is disclosed to rights holders, including information that "appears on the merchandise and its packaging and labels" as described in section 302, CBP is not aware of any prohibition that would prevent the rights holders from sharing the information with platform e-commerce companies or other third parties.

In addition, CBP has determined that section 302 does not provide authority to disclose information appearing on packing, which CBP defines as "all containers, exclusive of instruments of international traffic, and coverings of whatever nature, used in placing the merchandise packed ready for shipment to the United States" (19 CFR § 152.102(e)). Consequently, it does not authorize the disclosure of information to rights holders that is contained on or within the packing, *e.g.,* a "fulfilled by Amazon" (FBA) number, or an invoice or packing slip enclosed with the packing. Such information would be considered packing as opposed to packaging, and that distinction is salient in CBP regulations reflecting U.S. trade agreements. Specifically, the term "*packaging* materials and containers" is defined for Customs purposes in numerous provisions of CBP Regulations as meaning the "materials and containers in which a good is packaged for retail sale" (19 CFR part 181, appendix, part I, section II (the NAFTA Rules of Origin Regulations), emphasis added). However, the term "*packing* materials and containers" are defined as "materials and containers that are used to protect a good during transportation, but [do] not include packaging materials and containers" (*Id.,* emphasis added). CBP regulations matching this meaning for "packing" also comport with the United States–Korea Free Trade Agreement, the United States–Panama Trade Promotion Agreement, and the United States–Columbia Trade Promotion Agreement, all of which explicitly do not include the materials and containers in which merchandise is packaged for retail sale. We glean nothing in TFTEA or its legislative history to suggest disregarding the differentiation between "packaging" and "packing" consistently made in existing statutes and trade agreements. Consequentially, CBP does not have the authority in TFTEA or elsewhere to disclose to the right holders e-commerce platform data located on the package or within the package on an invoice, such as a "fulfilled by Amazon" (FBA) number.

Further section 302 does not provide explicit authority to disclose information appearing on packing, which CBP defines as "all containers, exclusive of instruments of international traffic, and coverings of whatever nature, used in placing the merchandise packed ready for shipment to the United States" (19 CFR § 152.102(e)). It does not explicitly allow for the disclosure of information to rights holders that is contained on or within the packing, *e.g.,* a "fulfilled by Amazon" (FBA) number, or an invoice or packing slip enclosed with the packing. [Note: As discussed above in the response to question 5, CBP has drafted a Notice of Proposed Rulemaking (NPRM) to implement sections 302 and 303 of TFTEA with respect to the seizure of circumvention devices and other copyright-infringing goods. The draft NPRM is currently within the interdepartmental review process.]

However, as noted above in our answers to questions 2 and 4, CBP has statutory authority beyond section 302 of TFTEA, including that provided by 15 U.S.C. § 1124 and 19 U.S.C. §§ 1526 and 1595a, that may provide authority for CBP to promulgate regulations to share e-commerce platform data located on the package or within it on an invoice with rights holders.

CBP has drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process.

CBP EFFORTS TO STOP COUNTERFEITS DIRECTLY SHIPPED TO CONSUMERS

Question. While CBP has a heavy focus on large shipments to identify and confiscate counterfeits, how does the agency deal with foreign-direct shipments of counterfeits to consumers and what is CBP's longer-term plan to deal with the continued growth of e-commerce and direct-to-consumer sales?

Answer. CBP currently treats small packages in the same way that it treats all cargo entering the United States. Advanced cargo screening data is available for shipments coming into express consignment facilities such as DHL, FedEx and UPS. A combination of automated targeting systems and CBP Officer evaluation leads to cargo exams and seizures.

CBP recently released an E-Commerce Strategy, which outlines a number of high-level goals that will allow CBP to adapt to the increasing number of small, direct-

to-consumer shipments. The goals that are outlined in these strategic plans include enhancing legal and regulatory authorities to better posture CBP and interagency partners to address emerging threats, enhancing and adapting all affected CBP operations to respond to emerging supply chain dynamics created by the rapid growth of e-commerce, driving private sector compliance through enforcement resources and incentives, and facilitating international trade standards for e-commerce to support economic prosperity. This new direct-to-consumer model includes new entities facilitating the purchase and movement of goods into the United States.

QUESTIONS SUBMITTED BY HON. ROB PORTMAN

Question. It seems that one new tool that might help facilitate information sharing between Federal agencies and the private sector in this space would be the use of Administrative Protective Orders (APOs). The International Trade Commission and the Department of Commerce successfully use APOs to facilitate confidential information sharing with interested parties and it seems that there may be opportunities to apply that model here. In the context of duty evasion and the Enforce and Protect Act (EAPA), I've heard from many stakeholders about how they want an APO process at CBP because of how useful it is in fostering the collaboration needed to tackle these problems.

Executive Assistant Commissioner (EAC) Smith, I understand the concerns about the lack of legal authority when it comes to APOs in the counterfeit goods space, but setting that aside for a moment—do you think that, as a practical matter, an APO may be useful to help facilitate information sharing when it comes to counterfeit goods or when it comes to duty evasion, as well?

Answer. CBP is of the view that an APO-like procedure would not be suitable to the border enforcement environment. APOs are used in distinct administrative proceedings of a legal nature, such as at the U.S. International Trade Commission (ITC) or at the International Trade Administration (ITA), Department of Commerce, to ensure that Confidential Business Information (CBI) that is disclosed to outside counsel (and not to interested parties themselves) is used only in the context of an administrative proceeding and not divulged to unauthorized persons. The APOs are effective because of the threat of sanctions, such as official reprimands, disbarment or referral to the U.S. Attorney, against those persons who sign on to the order but subsequently violate it.

Thus, for an APO process to be effective, CBP would also need to have the means of enforcing the order through sanctions of the sort described above. Furthermore, as distinct from APOs at the ITC or ITA, which are issued in respect of particular, clearly defined matters, the contemplated disclosure of information would occur on a regular basis. It is also not immediately clear how sanctions, which bind counsel in court-like settings, could be adapted to an operational setting. Consequently, it is our view that APOs would prove to be a thoroughly unsuitable vehicle for disclosing information.

QUESTIONS SUBMITTED BY HON. MARIA CANTWELL

Question. As the GAO report identifies, CBP does not proactively communicate with online marketplaces that have teams that work closely with the intellectual property rights center, brands, and law enforcement to keep counterfeit items off their sites. However, information sharing is critical.

What are the specific legal parameters for sharing information with e-commerce websites about counterfeit goods CBP seizes?

Answer. As discussed elsewhere, CBP's current IPR information sharing authorities, including section 302 of TFTEA, provide "authorized by law" exceptions to the Trade Secrets Act (TSA), permitting disclosures to trademark and copyright owners. As such, CBP does not disclose information concerning IPR-violative shipments to third parties such as e-commerce platform owners. Once information is disclosed to rights holders, CBP is not aware of any prohibition that would prevent the rights holders from sharing the information with platform e-commerce companies or other third parties.

Question. CBP is currently reviewing options for sharing additional information with rights holders and e-commerce websites. What is the timetable for this review?

Answer. CBP's review of options for additional information sharing with rights holders and e-commerce websites is ongoing.

Question. What are the differences between the information sharing rules for the CBP and ICE?

Answer. CBP is bound by the provisions of 6 CFR part 5 and the Trade Secrets Act (18 U.S.C. § 1905) and assumes that ICE, as a DHS component and as USG employees, is as well. CBP notes that it has promulgated regulations, set forth in 19 CFR part 133, governing the disclosure of information for purposes of IPR enforcement and that these regulations constitute a limited exception to the Trade Secrets Act. As a general matter, however, we note that if ICE were to obtain confidential information from CBP it would require CBP's consent to disclose the information to third parties.

Question. How is the relationship with the Intellectual Property Center working? In your view, is CBP getting sufficient information to properly do the job?

Answer. The relationship between CBP and the National Intellectual Property Rights Coordination Center (IPR Center) is one in which communication collaboration and information sharing continue to yield valuable outcomes. CBP has permanently staffed the IPR Center with a deputy assistant director and five full-time international trade specialists. This staffing allows the sharing of trade enforcement information among the 23 IPR Center partner agencies regarding IPR enforcement actions throughout the various ports of entry. Data is also shared to assist in civil and criminal cases.

Question. CBP and ICE coordinate with several other Federal agencies in their efforts to interdict the flow of counterfeit goods into the United States. As a part of this effort, CBP and ICE also work with rights holders to ensure that their trademarks and copyrights are recorded in the CBP online system. Also, CBP puts a priority on enforcing IP registered with the U.S. Patent and Trademark Office and the U.S. Copyright Office.

According to the GAO report, increasing the number of patents, trademarks and copyrights with the CBP was an important way that a rights holders can help CBP's enforcement efforts.

Given the benefits of registering patents, trademarks and copyrights with CBP, does the U.S. Patent and Trademark Office or the U.S. Copyright Office share information with the CBP?

Answer. Through its recordation process, CBP gives priority to the border enforcement of trademarks registered on the Principal Register of the U.S. Patent and Trademark Office and copyrights that are registered with the U.S. Copyright Office (or for which an application for registration has been submitted). Information concerning federally registered trademarks and copyrights is publicly available. Information on registered patents is also publicly available; however, it should be noted that in contrast with trademarks and copyrights, CBP does not record patents given that it has no authority to enforce patents except in the context of an exclusion order issued by the U.S. International Trade Commission.

Question. If so, what steps could be taken to improve the sharing of registrant information for new patents, trademarks and copyrights?

Answer. CBP conducts outreach initiatives to promote the recordation process and believes that this is the best and most effective means of increasing the number of recordations.

Question. Could the U.S. Patent and Trademark Office or the U.S. Copyright Office forms be adapted to provide simultaneous registration with the CBP?

Answer. The Copyright Office, the PTO and CBP previously studied the issue of simultaneous registration-recordation and concluded that it was not a viable option. There are well in excess of a million trademarks and copyrights registered with the PTO and the Copyright Office, most of which are at little or no risk of infringement by imported merchandise, *e.g.,* service marks, marks on the Supplemental Register, unknown and non-commercial works, etc. If all rights holders were offered the chance to record with CBP as part of the Copyright Office and PTO registration process, they might well feel compelled to record with CBP, thereby leading to a significant increase in recordations that would never be enforced, but for which CBP would nevertheless be responsible for monitoring, thereby diverting resources from the enforcement of recorded trademarks and copyrights that are far more susceptible to infringement at the border.

Question. CBP processed more $2.39 trillion in imports, 33.2 million entries and more than 28.5 million imported cargo containers. 250 million cargo, postal, and express consignment packages arrive through air travel. CBP plays a central role in coordinating with 23 agencies and ICE–HSI in the IPR Center. Through these efforts, you have helped to shut down counterfeit medicine and medical device websites, seized unsafe products ranging from automotive parts to toys, and prevented illegal imports via the mail of many counterfeited products. These efforts take an enormous amount of coordination. In your testimony, you discussed the need to collaborate with your partners, and stated that,

"One of the main challenges identified was the need for better data collection, automation, and a legal framework for sharing data."

Can you provide more detail regarding what legal framework is needed to improve your ability to share and collect data?

Answer. As discussed elsewhere, DHS has been taking "all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders" the two categories of information that the President specified in Executive Order 13785. This has included an ongoing evaluation of the extent to which CBP's disclosure of additional information to rights holders would involve any information that is of the type that is generally covered by the Trade Secrets Act (18 U.S.C. § 1905) and, with respect to any such information, whether Congress—in section 302 of TFTEA, 19 U.S.C. § 1628a, or otherwise—has granted CBP sufficient authority to disclose such information to rights holders. CBP is preparing a list of potential statutory changes that would bolster CBP's ability to enforce intellectual property rights at the border, to include improving the ability to collect and share data on e-commerce shipments. As part of this process, CBP is consulting with ICE and with private sector stakeholders both directly and through the Commercial Customs Operations Advisory Committee.

Question. What are the limitations of increased information sharing and data collection with non-government entities, such as e-commerce sites, rights holders, third party providers, etc.?

What are the concerns or downsides if any?

Answer. As discussed or referenced in questions 2, 4, 11, 17, 20, and 22, the primary concern presented is the Trade Secrets Act, 18 U.S.C. § 1905, a criminal statute barring the unauthorized disclosure by government employees of any confidential business information received in the course of their employment. Case law interpreting the Trade Secrets Act, which includes Supreme Court decisions and the Act's legislative history, demonstrates that it covers most commercial or financial data collected by any Federal employee from any source.

The current regulations governing disclosure at the detention stage and upon seizure are set forth in 19 CFR part 133, including section 133.21. These regulations currently limit CBP's disclosure ability to cases of suspect trademarks. At the detention stage, CBP can provide limited importation information to the right holder, including:

(1) The date of importation;
(2) The port of entry;
(3) The description of the merchandise;
(4) The quantity; and
(5) The country of origin of the merchandise.

CBP may disclose information "appearing on" the goods and its retail packaging in the case of trademark detentions, assuming the importer is unable to establish during the 7-day notice period that the suspect mark is not counterfeit. [Note: As discussed above in the response to question 5, CBP has also drafted an NPRM to implement sections 302 and 303 of TFTEA, so as to enable CBP to make copyright/DMCA detention disclosures; the draft NPRM is currently within the interdepartmental review process.]

Post-seizure, CBP may also disclose eight data elements to the right holder, which includes:

(1) The date of importation;
(2) The port of entry;
(3) The description of the merchandise;
(4) The quantity;
(5) The name and address of the manufacturer;
(6) The country of origin of the merchandise;

(7) The name and address of the exporter; and
(8) The name and address of the importer.

CBP is of the view that it would be beneficial to its enforcement efforts for additional information to be disclosed to trademark and copyright owners post-seizure/abandonment after an infringement determination is made, including the names and address of all persons involved in the purchase, sale, shipping and financing—to the extent known—of counterfeit and piratical merchandise imported into the United States.

In addition to the above-referenced NPRM, CBP has also drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process.

Also as discussed elsewhere, DHS has been taking "all appropriate steps, including rulemaking if necessary, to ensure that CBP can, consistent with law, share with rights holders" the two categories of information that the President specified in Executive Order 13785. This has included an ongoing evaluation of the extent to which CBP's disclosure of additional information to rights holders would involve any information that is of the type that is generally covered by the Trade Secrets Act (18 U.S.C. § 1905) and, with respect to any such information, whether Congress—in section 302 of TFTEA, 19 U.S.C. § 1628a, or otherwise—has granted CBP sufficient authority to disclose such information to rights holders. CBP is very mindful of the protections and restrictions imposed by the Trade Secrets Act as most of the information collected by CBP falls under the category of confidential business information protected by that statute, which must remain protected in the trademark and copyright enforcement context until either a violation is found or a disclosure is necessary to get help in proving such a violation exists.

Question. The U.S. Coast Guard participates alongside CBP, ICE, USDA and several other Federal agencies in multi-agency strike force operations at our ports each year. These joint strike force operations require a great deal of planning and coordination and they often yield substantial results.

As a part of the overall interdiction of counterfeit goods, how could more frequent and better targeted joint operations reduce the inflow of counterfeit goods?

Answer. More frequent and focused joint operations in anti-counterfeiting and intellectual property rights enforcement certainly increases the number of seizures, and has a similar deterrent effect to some degree. Moreover, one additional benefit of joint operations in anti-counterfeiting is the public educational aspect. Only by reducing public demand for counterfeit items in general can we truly see a significant reduction in the problem. Well-publicized joint operations can help in this way.

Question. These large operations require a great deal of transparency and communication among the agencies involved. Have you looked at these operations to see how this cooperation and communication could be better integrated into your standard operating procedure?

Answer. Often, the same CBP Officers who work on joint operations with partner agencies also work in anti-counterfeiting and intellectual property rights protection. There is a natural knowledge transfer and experience building process in the operational planning, communications, and transparency of joint operations.

We agree that analyzing all joint operations with the goal of finding best practices and efficiencies to be shared CBP-wide is an activity that CBP continues to undertake.

Question. The Coast Guard has a presence at every port. In addition to increasing information sharing between the CBP and ICE, have you examined the benefits from joint trainings with the Coast Guard?

Answer. Both the Coast Guard and CBP are frontline border security agencies. Joint training in the mission areas of anti-smuggling, illegal immigration, secure and safe cargo operations, and other border activities occurs frequently and is highly beneficial. However, as the Coast Guard has not had a significant role in anti-counterfeiting or intellectual property rights enforcement, joint training in those activities has not been a priority for field personnel.

Question. In the Trade Facilitation and Trade Enforcement Act of 2015 (TFTEA), section 303 called for a new regulation regarding the disclosure of information upon seizure of circumvention devices to be promulgated within a year of the enactment

of the legislation. This February marked 2 years since the passage of TFTEA and the regulation has yet to be promulgated. Circumvention devices are used to break the security of hardware in order to access illegal copyrighted content typically downloaded from the Internet. It is important for CBP to share information with businesses that are harmed by circumvention devices when they seize those devices.

Why has the promulgation of this regulation been so significantly delayed?

Answer. CBP has drafted a Notice of Proposed Rulemaking to implement sections 302 and 303 of TFTEA. The NPRM is currently within the interdepartmental review process. Also, as section 303(b) of TFTEA was the only subsection requiring the prescription of regulations for circumvention device seizure disclosures, CBP had concerns about issuing just that portion of TFTEA without the broader circumvention device regulatory context drafted in the NPRM currently in the interdepartmental review process. Without such context, the public may have been confused as to how such disclosures fit into CBP's circumvention device enforcement regime as changed by TFTEA. As such, the current package provides this context in a way that should empower those injured by the circumvention violations that TFTEA prohibits.

CBP has also drafted an NPRM to amend its regulations to disclose to trademark owners, when merchandise has been voluntarily abandoned, the same comprehensive importation information that is disclosed when merchandise bearing a suspected counterfeit mark has been seized. The draft NPRM is currently in the interdepartmental review process.

Question. Please provide us with an update on the promulgation of the regulation required by TFTEA section 303. When will the promulgation of this regulation be completed?

Answer. As noted above, the NPRM is in the interdepartmental review process.

QUESTIONS SUBMITTED BY HON. BILL NELSON

Question. What sort of products do you see the most come in as counterfeit goods and what countries do they normally come from?

Answer. The most commonly seized items are wearing apparel and accessories such as team jerseys and belts. Forty-six percent of all goods seized come from China and 32 percent come from Hong Kong. For extensive information on our IPR seizures can be found at *https://www.cbp.gov/trade/priority-issues/ipr/statistics.*

Question. Have you shared information about problematic countries or types of products, as referenced above, with anyone at the White House or in USTR?

Answer. CBP works closely with the partner government agencies, including USTR, to help with the development of the annual Special 301 Report and the Notorious Markets List. Through this interagency collaborative process, CBP shares concerns about counterfeit issues from relevant economies. These concerns are discussed with the interagency at length and addressed in these reports to Congress.

In addition, CBP recently provided IPR seizure statistics for China and Hong Kong to the National Economic Council.

Question. If so, what was their response? If not, why not?

Answer. The National Economic Council is currently reviewing the information that CBP provided. Additionally, as mentioned above, CBP's input is included in the annual Special 301 Report and the Notorious Markets List.

PREPARED STATEMENT OF HON. RON WYDEN,
A U.S. SENATOR FROM OREGON

This morning, the Finance Committee meets to discuss the challenge of protecting consumers from counterfeit goods. And, I am glad that we are having this discussion, which is overdue in my book. In addition, I hope that this committee will soon hold hearings on the administration's many trade activities—including the steel and aluminum investigations and potential tariffs, the NAFTA renegotiations, and the investigation of China under section 301.

On counterfeit imports, any discussion of this issue has to begin by recognizing that over the last few decades, the Internet has transformed virtually every facet of our economy. It is the shipping lane of the 21st century. And people now take

it for granted, but it's a miracle of the modern world that a small business in Oregon is able to reach consumers almost anywhere, anytime. No longer does expanding your customer base mean investing in bricks and mortar.

Wildfang is a socially conscious Portland clothing company that was founded by women and run by women. They have two stores in Portland, but what's really driving sales, according to founder Emma McIlroy, is online sales. A full 70 percent of their business happens online, and that's where their growth is happening. This is a company that seized the opportunity to sell around the world via the Internet, and now has 25 employees.

But as with any economic transformation, the upside comes with new challenges. That includes the chance that when you buy something online, it could be a fake.

It's up to the Federal Government to make sure our approach to combating counterfeits isn't stuck in the 20th century. These days, when you talk about cracking down on counterfeit goods, you're no longer talking about stopping the guy selling fake purses out of his trunk. You're talking about illegitimate products passed off on even the most streetwise consumers, often because they're mixed right in with the genuine products people want. Many of those fakes pose serious dangers. Makeup and food and beverage containers made with dangerous chemicals. Electronics that pose a fire hazard. Toys that are unsafe for children.

The number of small packages coming into our country has surged, and Customs and Border Protection has a major role to play in identifying counterfeits and stopping them before they enter our marketplace. But unfortunately, CBP is too often playing catch up ball tracking these fake products down.

After conducting a recent study of this exact issue requested by Chairman Hatch, the Government Accountability Office recommended a set of policy updates to have CBP work more closely with the private sector. Those recommendations included expanding CBP's authority to notify online sales platforms when they've got products on their hands that might be fake.

You might hope that would set the wheels in motion to get those policies in place. But CBP responded to GAO late last year by claiming it would take until this upcoming September to determine if that additional authority was really necessary.

Over the last few years, this committee has put a lot of sweat equity into policies that strengthen the enforcement of our trade laws and protect American consumers and workers. Senator Hatch and I authored the Trade Facilitation and Trade Enforcement Act of 2015 that put in place important new tools for CBP to detect and prevent counterfeits, including by sharing information about counterfeit imports with rights holders. So in preparation for this hearing, committee staff from both sides, sat down with CBP to dig into this issue.

My staff asked, "Does CBP need more authority to crack down on counterfeits?" CBP said they didn't know. When asked when they would know, CBP said they didn't know when they would know.

It's concerning to me that we were unable to get a straight answer on a matter like this from the agency at the heart of our efforts to protect American consumers from counterfeit goods. So I'm going to give CBP another chance to answer these questions today.

But let's also recognize that getting this right isn't going to be as simple as putting a few more policy tools in CBP's kit.

Year after year, administrations have fallen short in hiring enough officers—blue uniforms—to fulfill the critical need of protecting U.S. consumers and businesses from illegal and unfairly traded goods. It's a tough job CBP's got on its hands, working with other law enforcement agencies and foreign governments to go after the source of these problems. If the administration is focused solely on hiring an army of Border Patrol agents, I don't see how that is going to build up CBP's capacity to deal with these counterfeit challenges. So the Congress and the administration need to guarantee that CBP has the resources it needs to combat counterfeiters, and that it actually follows through.

This is a matter of protecting families from harmful products and preventing rip-off artists from undercutting the American brand. It's essential that the Federal Government take the right approach with fresh policies that take the realities of our modern economy into account.

I look forward to hearing from our witnesses on these issues today.

COMMUNICATIONS

ALLIANCE FOR SAFE ONLINE PHARMACIES
1050 K Street, NW, Suite 400
Washington, DC 20001
Libby.Baney@BuySafeRx.pharmacy
Direct: (202) 312–7438

March 20, 2018

Hon. Orrin Hatch, Chairman
U.S. Senate
Committee on Finance
Dirksen Senate Office Building
Washington, DC 20510–6200

Hon. Ron Wyden, Ranking Member
U.S. Senate
Committee on Finance
Dirksen Senate Office Building
Washington, DC 20510–6200

RE: Statement for the Record from the Alliance for Safe Online Pharmacies (ASOP Global) on the full committee hearing on "Protecting E-commerce Consumers From Counterfeits"

Dear Chairman Hatch and Ranking Member Wyden:

Thank you for considering the Alliance for Safe Online Pharmacies' (ASOP Global) statement for the record in response to the U.S. Senate Committee on Finance hearing "Protecting E-commerce Consumers From Counterfeits" on Tuesday, March 6, 2018.

ASOP Global is a nonprofit organization dedicated to addressing the public health threat posed by illegal online prescription drug sellers. Our work focuses on research, consumer awareness, advocacy, and international engagement. With over 85 member organizations worldwide, ASOP Global is active in the United States, Canada, Europe, India, Latin America and Asia. For more about ASOP Global please visit *www.BuySafeRx.Pharmacy.*

We would like to thank the Committee for its leadership on addressing the issue of counterfeit products entering the United States. Counterfeit drugs, including those marketed as controlled substances, have been linked to serious injury and even death. As you know, the significant influx in counterfeit, falsified and substandard medicines into the country remains a critical patient safety and public health issue.

According to U.S. Customs and Border Protection,[1] counterfeit pharmaceutical products now account for nearly 6% of all counterfeit product seizures in the U.S. and totaled nearly $70 million in fiscal year 2017. Globally, the World Health Organization estimates that the costs incurred from counterfeit pharmaceutical products are approximately $75 billion per year.[2] U.S. seizures and international operations, such as INTERPOL's Operation Pangea, continue to illustrate the need for comprehensive and coordinated efforts to ensure counterfeit medicines do not continue to make their way into American households.

Recently, Members of Congress and several federal agencies have called attention to the increase in online sales of prescription medicines and illicit narcotics, such as fentanyl and carfentanil, shipped to the U.S. through the Postal Service.[3] Senate

---

[1] *https://www.cbp.gov/sites/default/files/assets/documents/2018-Feb/trade-fy2017-ipr-seizures.pdf.*

[2] *http://business.financialpost.com/opinion/they-cost-us-billions-and-they-can-kill-counterfeit-drugs-are-invading-canada.*

[3] *https://www.hsgac.senate.gov/subcommittees/investigations/hearings/combatting-the-opioid-crisis-exploiting-vulnerabilities-in-international-mail.*

investigators on the Senate Permanent Subcommittee on Investigations (PSI) have identified hundreds of illegal online drug transactions in over 40 states, adding up to $230,000 worth of fentanyl—with a street value of over $750 million—from just six online seller s. This is not surprising given the size and sophistication of illegal online drug sellers often posing as legitimate online pharmacies. ASOP Global Board Member LegitScript has found there are roughly 35,000 active online drug sellers operating at any one time, and the National Association of Boards of Pharmacy (NABP) reports that 96% of these sites are unsafe and illegal, failing to comply with state and federal laws or pharmacy practice standards. What is more, a February 2018 report by NABP found that more half (54%) of the online drug sellers they analyzed offered controlled substances, and 40% offered one or more of the drugs frequently counterfeited with fentanyl.[4] This puts millions of Americans at risk of receiving dangerous counterfeit or otherwise illegal and unsafe medications, often shipped into the U.S. from foreign sources to patients without requiring a prescription.

Given the danger posed by counterfeit prescription drugs (including fentanyl) sold online, it is crucial the U.S. does more to reinforce international shipping standards. The failure to track and stop shipments containing illegal prescription and synthetic drugs from rogue online pharmacies, as well as failing to prepare for the increase in international shipments due to the lack of advanced electronic data, will only continue to put Americans at risk and worsen the nation's opioid epidemic. ASOP Global appreciates the Administration's effort to encourage foreign jurisdictions to provide advance shipment data, but feels more must be done. ASOP Global supports enactment of the Synthetics Trafficking and Overdose Prevention (STOP) Act as well as additional Administration actions to crack down on illegal shipments of counterfeit or otherwise illegal medicines into the U.S.

Recently FDA Commissioner Scott Gottlieb moved to improve the agency's ability to screen for illegal prescription and illicit drugs at several international mail facilities. He doubled the staff responsible for package inspections and called for further expansion this program.[5] ASOP Global support this and otherFDA efforts to crack down on illegal online sellers and is pleased to see the Administration focus more resources on stopping dangerous counterfeit and otherwise illegal medicines at the border.

In addition to the issue of stopping illegal prescription drugs via international mail facilities, as Senators Grassley, Feinstein, Klobuchar, Kennedy and Whitehouse recently observed,[6] online platforms and marketplaces also have a key role to play in stopping the deadly supply of counterfeit and otherwise illegal medicines from reaching Americans. A recent study[7] published in the *American Journal of Public Health* found widespread use of Twitter, Facebook and YouTube by illegal online pharmacies to market and sell fentanyl, oxycodone and other highly addictive, often deadly controlled substances to U.S. consumers, in direct violation of federal law. Moreover, online platforms and marketplaces make it easy—even by accident—to find illegal sources of prescription and illicit drugs online. For example, an innocuous search for *e.g.* "Follistim (an infertility drug) online" or "fentanyl online" yields dozens of top-page search results for illegal sites offering medicines without a prescription shipped through the USPS. Rather than offering up illegal online drug sellers on page one—including Canada Drugs.com—which has been indicted and recently pled guilty to selling counterfeit medicines to Americans[8]—is in the public interest for online platforms and marketplaces to return results that lead Americans to legitimate sources of medicine and information in response to innocuous queries. We encourage this Committee to consider ways to further encourage online platforms and marketplaces to promote legitimate sources of medicine and health information as part of your ongoing efforts to protect Americans from counterfeit goods sold online.

Finally, ASOP Global supports the recommendations outlined in the Government Accountability Office's January 2018 Intellectual Property Report,[9] including strengthening the detection of IPR-infringing goods, engagement with international

---

[4] *https://nabp.pharmacy/wp-content/uploads/2018/02/lnternet-Drug-Report-Feb-2018.pdf.*

[5] *https://www.apnews.com/6de59e7d620b4a75b605e60580blc569/FDA-chief-wants-more-mail-inspectors-to-stem-opioid-influx.*

[6] *https://www.grassley.senate.gov/news/news-releases/grassley-feinstein-colleagues-urge-tech-companies-clamp-down-illegal-online-drug.*

[7] *https://www.ncbi.nlm.nih.gov/pubmed/29048960.*

[8] *https://buysaferx.pharmacy/news-release-statement-in-response-to-case/.*

[9] *https://www.gao.gov/assets/690/689713.pdf.*

partners, and launching localized pilots and port-specific initiatives. Increased resources focused towards the U.S. agencies responsible for this oversight, such as Customs and Border Protection, Homeland Security Investigations, Federal Bureau of Investigations, and others, are necessary.

The Alliance for Safe Online Pharmacies thanks you for considering this statement and stands ready to assist the Committee in your continued work on important public health and safety issue.

Respectfully,

Libby Baney
Executive Director

ASMODEE NORTH AMERICA, INC.
1995 County Road B2 West
Roseville, MN 55113
https://www.asmodeena.com/en/

June 26, 2018

U.S. Senate
Committee on Finance
Dirksen Senate Office Bldg.
Washington, DC 20510–6200

Honorable Committee Members:

We write today on behalf of our firm, Asmodee North America, Inc. (Asmodee), in order to inform the Committee and the American public about Asmodee's experience with online counterfeit sales of our products. Asmodee supports our government in finding ways to better inform American consumers of the dangers presented by counterfeit goods. Asmodee also seeks to assist the U.S. Government in protecting intellectual property rights by curtailing the illegal sale of counterfeit goods through e-commerce sites.

About Asmodee

Asmodee is a leading global creator, publisher, and distributor of board games, card games, family games, hobby games, and digital games. We tell countless stories through our games. In fact, our trademarked motto is: "Great Games . . . Amazing Stories."

A global corporation, the Asmodee Group operates offices in Belgium, Canada, China, France, Germany, Italy, the Netherlands, Scandinavia, Spain, the United States, and the United Kingdom. Our North American headquarters is situated in Roseville, Minnesota, where we also operate 2 major creative studios. We also operate in Texas, Virginia, California, Pennsylvania, and Washington State. Asmodee North America, Inc. employs roughly 250 people in the U.S.

Asmodee either directly, or through affiliates, owns the publishing brands *Asmodee Games, Catan Studio, Days of Wonder, Fantasy Flight Games, Pearl Games, Plaid Hat Games, Rebel, Space Cowboys,* and *Z-Man Games.* Through these publishing studios and our third-party partners, Asmodee is the originator of such best-selling titles as *A Game of Thrones: The Board Game, Carcassonne, Catan, Dixit, Ticket to Ride, Pandemic, Rory's Story Cubes, Seven Wonders, Spot It!, Splendor, Star Wars: Destiny, Star Wars: X-Wing,* and hundreds more. Many of these products sit at the very top of best-selling charts for toys and games globally.

Asmodee invests a tremendous amount of passion, talent, time and expense in building these products. We spend a significant amount of energy and capital in building the reputation and value of our brands, including our corporate identity. Because of our solid reputation, Asmodee enjoys strong, long-time licensing partnerships with significant intellectual property (IP) holders such as Disney, HBO, George RR Martin, NBC Universal, Middle-earth Enterprises, Lucasfilm, and others.

Our firm has grown to become a cultural force. You frequently see Asmodee games in classrooms, the news, and in stories told on television and in film. You find our IP in merchandise and other forms of licensing. We are the preeminent game-specific (as opposed to toy) company in the United States, if not the world.

Impact of IP Counterfeiting on Asmodee and its Consumers

With success comes challenges. During the last 2 years in particular, counterfeit sales in the e-commerce marketplace have explosively increased. Sales of counterfeit Asmodee games have negatively impacted our brands, reputation, relationships, business infrastructure, revenue, profit, and value. In a very material way, this recent surge of counterfeit Asmodee products in the U.S. marketplace directly threatens the viability of our company and our industry, as well as the safety and satisfaction of our consumers.

Counterfeiting activities infringe upon nearly all our intellectual property, whether held by copyright, trademark, or common law rights. Naturally, they disproportionally affect our most popular titles. This IP piracy hurts everyone in our supply, publishing, and distribution chains. It also impacts consumers.

While consumers may occasionally purchase a counterfeit product directly from a brick-and-mortar game store, encounters with inauthentic goods occur most commonly on e-commerce sites—large, small, and in between. Counterfeit games frequently appear for sale on "third-party retailer" sites inside the largest and most prominent of e-commerce platforms.

Counterfeit goods infect the "co-mingling" warehouse practices of large e-commerce platforms, where goods from its vendors, as well as third-party sellers, may be stored in the same warehouse SKU location for efficiency and geographic stock balancing. These "co-mingled" counterfeit goods may later be pulled and sold by the e-commerce retailer on its own account, or to service a sale on behalf of a legitimate third-party seller who originally shipped authentic stock to the e-commerce warehouse.

This counterfeit trade creates uncertainty about the nature, quality, and safety of our products, especially those sold through e-commerce platforms. Few counterfeit game components receive positive reviews. Many are unfit for purpose. Many receive scathing reviews. Most consumers have no idea that these reviews refer to inauthentic goods, and in most instances neither does the reviewer.

Counterfeit products place the consumer at a safety risk. While it is unlikely that counterfeit games get tested for safety, Asmodee spends extensively to test its products in order to meet mandated U.S. and C.E. safety requirements, including testing for substances such as phthalates, lead, and other toxic materials. We believe that counterfeiters rarely invest in testing their source materials and are likely to use toxic materials to lower their cost of manufacturing. In our view, such unsafe manufacturing and distribution activities endanger the public safety.

Commerce in counterfeit games materially affects price stability, for automated "pricing robots" calibrate their offers in response to the online availability and listed prices of discounted product. Artificial price plunges—unwanted by even the very e-commerce platforms driving the system—result in a distortion of the marketplace, crushing profits and undermine a healthy free trade system. This directly impacts all retailers, distributors, and publishers. This erodes investment and developmental incentivization at every level, threatening to rob the consumer of the potential product options otherwise found in a fertile marketplace.

Commerce in counterfeit games also tarnishes public confidence in our products and brands. As noted, consumers reviewing substandard counterfeits often innocently attack products in the most public and persistent online forums. This powerful "misinformation" creates further confusion for their fellow consumers.

Evidence of IP Counterfeiting

Asmodee has collected a very substantial number of physical counterfeit samples. We have photographic evidence of the products, receipt dates, transaction information, and shipping labels. U.S. Customs and Border Patrol (USCBP) has provided us with documentation of their sporadic seizures of counterfeit games, each depicting an intended e-commerce platform warehouse destination.

Asmodee has also compiled data on numerous consumer reviews explicitly calling out quality issues directly attributable to counterfeit games. These reviews clearly depict (*e.g.,* via grading/stars) an alarming deterioration in customer confidence. They document the damaging misperception borne out of a marked increase in the circulation of counterfeit merchandise.

Asmodee has also gathered statistical evidence that correlate our sales, pricing, reviews, and our own customer service incidents, evidencing the impact and existence of substantial counterfeiting activity by many third-party sellers. Overall, such evi-

dence indicates that illegal counterfeit copies of our products fill many e-commerce warehouses.

The e-commerce distribution methods that mask counterfeiting also masks other criminal activity in e-commerce, even on the largest platforms. Asmodee has evidence of stolen products, procured from legitimate sellers with stolen credit cards, being sold on e-commerce sites. Here, consumers face the prospect of unwittingly purchasing stolen goods.

Re: May 30, 2018 Questions from the Senate Committee on Finance

Given our experience wrestling with the damage wrought by counterfeit games sold through e-commerce channels, Asmodee offers the following thoughts in response to the Committee's questions of May 30, 2018.

For the avoidance of doubt, Asmodee is not an Internet platform. Asmodee is a content provider and product originator. Asmodee carefully regulates its own product development, testing, and manufacturing channels. We sell our own legitimate products directly to trade and to consumers. So here, we only address questions—or portions thereof—relevant to our business model.

1. What types of remedial measures do you provide to U.S. consumers who may have unintentionally purchased a counterfeit good through an e-commerce platform?

Asmodee only sells its own genuine games to trade and consumer customers. Still, we stand by our products and brands. Thus, we are sometimes forced to replace counterfeit goods, or parts thereof, purchased by consumers from e-commerce platforms. This is particularly the case when consumers cannot obtain recourse from the e-commerce vendor as in the case of counterfeit games purchased as gifts and opened after the allowed return period.

To the point of remediation, one must ask first "who is accountable" before one can contemplate the nature or scope of the remediation.

While Asmodee does its best to help affected consumers, we offer that it is not fair for the rights holder to compensate consumers for the counterfeiting of its own brands.

Many e-commerce operators take no accountability, claiming "Fair Harbor" under the DMCA. Others may issue refunds to consumers who discover counterfeits. However, we believe this cost is ultimately recharged to the authentic vendors in the form of common "damage assessment co-ops" vendor fees, and thus ultimately to the consumer.

Trying to hold third-party sellers accountable has proven near-impossible. Due to the ease of becoming a third-party seller on even the largest e-commerce platforms, the great majority of bad actors provide false addresses and untraceable email accounts. Our understanding is that many bad actors may not even be based in the U.S., but that many are in China.

Further, third-party sellers may be held falsely accountable for selling counterfeit goods whenever the e-commerce operator "co-mingles" goods from different sellers and vendors, as the e-commerce operator inadvertently pulls a co mingled counterfeit copy to fulfill the third-party seller's transaction.

Following is a consumer review of a counterfeit *Catan* game on the largest e-commerce site in the country presented on a leading e-commerce platform as a "Top customer review" (on June 19, 2018):

Customer Review

2½ ★s I loved the game, but the board was in terrible condition.
By Joshua Caleb Stephenson on May 29, 2017

Verified Purchase

After playing this game with some friends, I absolutely loved it and wanted to buy my own game. It arrived yesterday and when I opened it up the quality of the game was in terrible condition. The board edges don't even fit together property making the game hard to setup and the hexagons are poorly cut and do not fit inside properly. I have to force the sides and hexagons in to get them to stay together. Some of the hexagons are printed poorly as well as you can see in the pictures. The pieces that came with it were in terrible condition as well, several roads were chipped and looked like they were cut in half and several of the house/cities were chipped and don't even stand up. I also was sent a yellow set of pieces which is supposed to be orange, and the yellow set was missing 3 roads as there is supposed to be 15 roads

per color. I was looking forward to playing this game, but the board set I was sent was in terrible condition and made me feel like I got ripped off.

I will update this and let you all know if I am able to get a replacement.

Certainly, Joshua was injured in this case and should be remediated. However, who will remediate the 35 people who found this review "helpful" (not to speak of those who read the review but did not click the "helpful" button)? These people are now more likely to be making a misinformed purchasing decision.

One must also recognize that, as stated earlier, most consumers are not aware that they've received and are consuming a counterfeit product, such as in the example above. Most counterfeit goods are either unsafe, or of lower quality than authentic product. The results create a negative impact on our society, our businesses, our safety, and our happiness. In such a case, the consumer cannot be remediated (as he/she does not know of the injury). In our view, while remediation is important, the solution to the e-commerce counterfeiting problem lies in prevention, starting with a clear assignment of accountability.

The simple answer to the question above is that, clearly, if a consumer has bought a counterfeit product, he/she should be able to return that product at no cost to him or herself.

2. What types of remedial measures do you provide to rights holders who find that counterfeit goods are being sold through an e-commerce platform?

Asmodee typically is the aggrieved rights holder whose IP is damaged when consumers purchase a counterfeit Asmodee game through an e-commerce platform.

3. In what circumstances does your organization come into physical contact with counterfeit products sold and delivered to consumers?

Asmodee receives actual counterfeit goods when consumers or trade customers send them to us, sometimes asking for compensation or replacement. When we suspect that someone is selling counterfeits online, we will test-purchase the goods as part of our investigation and policing process. When USCBP notifies us that they've seized suspected counterfeit goods at a U.S. port of entry, we might pay the requisite fee to obtain those counterfeit goods as part of our investigation and policing program.

4. What services, tools, protections, and assistance do you provide consumers and rights holders with respect to the sale of counterfeits?

For select products, Asmodee will provide a guide or guidelines detailing how a customer can determine if a product is a genuine Asmodee game. We show customers how they might identify counterfeits by examining the product or, especially relevant to e-commerce, how they might review the product's depiction or description, or the nature and circumstance of the sales offer.

As a rights holder and licensee of intellectual property, we try to protect ours and our licensors' rights by policing counterfeiting and standing behind our goods. This requires enormous investment, for we must police our supply chain from point of final consumer sale back through to the point of manufacture. We also find ourselves supplying consumers with genuine products or parts in return for counterfeit products or parts.

We also may, when we find such reviews, comment on online consumer reviews where we suspect a consumer may have received a counterfeit game.

5. Please explain what you feel are some of the biggest risks counterfeit goods currently pose e-commerce consumers?

They damage consumers' faith in otherwise reputable products and brands. They damage legitimate businesses and business infrastructure. They create tremendous confusion, anxiety, and wasted time. As in the case of counterfeit gifts, they may harm personal relationships. Regarding toxic components, they may provide a direct and material threat to consumer safety.

The rampant undermining of intellectual property rights inherent to counterfeiting will do tremendous damage to creative artists, content businesses, and to innovation in general. This could have a negative impact for both current and future generations.

6. What have you done to curtail those risks and what have you done to inform consumers of those same risks, which may not be known to the consumer?

Besides investing in material and outreach educating consumers about genuine Asmodee products, we are investing in manufacturing techniques, packaging, and game components that help deter counterfeiting, and help customers more easily identify genuine goods. Asmodee also polices the marketplace by searching for counterfeits offered through e-commerce and, wherever possible, works with sellers to shut down counterfeit offerings and sites/pages operated by counterfeiters.

That said, being a content and product originator, not an e-commerce platform, Asmodee does not often come into direct contact with the consumer at the point of purchase, as most of our products are sold through wholesale channels.

7. Do you engage with foreign governments to curtail the proliferation of counterfeits? If so, what types of activities and coordination have proven successful? What efforts have not been successful?

Asmodee always operates in accordance with the rule of law, regardless of venue. We register our copyrights and trademarks domestically and overseas, wherever appropriate and feasible. We occasionally seek recourse against counterfeiters via domestic and foreign courts. Our success directly depends on the strength of the particular foreign nation's IP laws and judicial system, and the associated costs.

8. To what extent do you facilitate delivery, storage, processing, and purchases of goods on your platform?

Asmodee does not operate an Internet platform.

Asmodee only sells its own genuine game products to trade customers and consumers. We police the development, testing, and manufacturing of all our products. This process retards IP theft at the point of manufacture. We then police the shipping, delivery, storage, and commercial sale of all of our products. We carefully examine returns in order to prevent the introduction of counterfeits into our warehouses.

9. Which inflection points in the e-commerce purchasing/selling process have you found most critical to intervene in to prevent and/or curtail the distribution of counterfeit goods?

We work with trustworthy suppliers who respect our IP, as well as all applicable quality and safety standards. These suppliers must use tested methods and components, maintaining secure manufacturing facilities and processes. Asmodee will regularly inspect third-party manufacturing facilities, either with our own staff, or by hiring third-party auditors.

We also seek to work with trusted trade customers, distributors, and retailers who are respectful of our IP and the needs and interests of our consumers. They must operate transparently enough to ensure that counterfeit goods do not inadvertently circulate through their warehouses or sales channels. In most cases, this requires that our trade customers only order Asmodee products directly from Asmodee. They must also police their own ordering, storage, and sales systems to combat the co-mingling of counterfeit goods or circulation of counterfeit products. With leading e-commerce platforms, on most accounts, this is not the case.

In our view, the critical points of inflection lie at (a) the point of procurement of products by e-commerce platforms, (b) the vetting and authentication of third party sellers on these platforms, and (c) the co-mingling of inventories from multiple vendors/sellers in e-commerce companies' ware houses.

Asmodee has sought, without luck, to partner with a leading e-commerce platform and assist in their vetting of accounts who wish to sell Asmodee's products on that platform. We've created unique software to securely identify our known authorized sellers, and we've offered to visit warehouses to identify counterfeit goods. All such suggestions were rejected by the platform. An explanation for these rejections has frequently been that our proposed solutions are "not scalable." We interpret this as meaning they are "too expensive."

Prior to the enactment of the "Fair Harbor" DMCA rule, retailers were held accountable for what was sold in their stores and responsible for vetting their vendors, whether they be brick-and-mortar or online retailers. Both consumer and vendor alike assumed that retailers stood by their wares and their desire to sell authentic goods. However, with the advent of online anonymity, easy access to consumers via e-commerce platforms, and the lack of realistic accountability by e-commerce platforms under "Safe Harbor," such trust is being materially eroded.

E-commerce operators take fees and commissions (often between 15–30% of proceeds) of third-party sales channeled through their platform, whether for legitimate or illegitimate goods. The enormous volume of counterfeit sales bolsters fixed cost absorption, profit, and cash flow of the e-commerce platform. Low online pricing of illegitimate goods boosts the e-commerce plat form's traffic volume, data gathering, and "add on" sales. We submit to the committee this happens at the expense of those retailers who care about supply vetting, those retailers who are not afforded impunity from counterfeit product trafficking by "Safe Harbors," and the honest creators of authentic products, and IP rights holders.

Despite their obfuscating public commentary, online e-commerce platforms significantly benefit from illegal counterfeiting activity and their lack of accountability, implicitly or not.

10. Have there been instances where genuine goods sold on your platform are intermingled and/or comingled with counterfeit goods: Can you provide an example?

Asmodee does not operate an Internet platform.

We have no evidence of counterfeit products being mixed with our own manufactured inventories. However, we have many examples and direct evidence of consumers having purchased counterfeit Asmodee products, sourced from so-called "comingled" inventories, facilitated by e-commerce platform operators.

11. How do you coordinate with rights holders to verify whether goods sold over your platform are genuine?

Asmodee does not operate an Internet platform.

As an IP holder and licensee, we only sell our own genuine goods. We ask our trade customers to order Asmodee products exclusively from Asmodee or through an Asmodee-authorized distributor.

12. In what ways do counterfeiters evade actions you have taken to prevent counterfeits on your platform or using your services?

Asmodee does not operate an Internet platform.

We sell only our own genuine Asmodee goods to customers, and we ask our trade customers to only purchase Asmodee products from Asmodee or an Asmodee-authorized distributor.

Instead, it is our trade customers' e-commerce platforms that prove most vulnerable to exploitation by counterfeiters. Counterfeiters evade our policing efforts by taking advantage of these e-commerce platform's lack of transparency, unwillingness to share data with rights holders, and the lack of accountability afforded to e-commerce platforms by the Fair Harbor DMCA standards.

When Asmodee does not have full transparency from an e-commerce platform customer on counterfeiting issues, whether due to its stonewalling or declared inability to address our concerns, we all suffer. It has been our experience that the largest e-commerce platforms refuse to provide effective solutions to the counterfeiting and stolen goods sales done on their websites. In our practical experience, extended brand management "tools" by e-commerce platforms are largely inadequate and provide solely reactive solutions.

At the same time (and quite maddeningly), e-commerce platforms continue to collect transaction fees from every illegal sale. They enjoy fixed cost mitigation from storage cost fees charged to bad-actor third-party sellers. They derive a substantial advantage from website traffic spurred by the impossibly low prices of counterfeit and stolen products. They work with impunity under the DMCA. We submit that the lack of collaboration and transparency by the largest e-commerce platform on this issue to-date enables and effectively aids and abets illegal behavior.

13. After a suspected counterfeit distributor has been identified—whether by your company or a third party—what steps do you take, if any, to verify claims of counterfeit distribution?

Asmodee checks to see whether the distributor has purchased goods from Asmodee or an Asmodee-authorized distributor. We seek photographic evidence of the character of the suspected goods. We may also obtain physical samples. We have considered hiring private investigators, and to submit the case to the proper authorities.

14. What is the process, if any, for removing a suspected counterfeit distributor from your platform?

Asmodee does not operate an Internet platform.

We seek removal of suspected counterfeit distributors from our customers' platforms by providing our customers with swift notice and clear evidence of counterfeiting. We employ exhaustive and expensive manual and automated policing assistance to take down sites operated by counterfeiters within and outside our distribution network.

We have exhaustively tried to work with the largest e-commerce platform on preventive measures, but without success.

15. After removal, what processes does your company have in place, if any, to prevent a counterfeit distributor from regaining access to your platform and subsequently U.S. consumers?

Asmodee does not operate an Internet platform.

We request that our e-commerce platform customers immediately deny the violating seller from selling our goods. However, in some instances it is the e-commerce platform itself selling counterfeit goods, due to procurement from illicit vendors, or in fulfilling their transaction from co-mingled inventories.

As it is trivial for anyone to create a new seller account on most e-commerce platforms under assumed/fake names, using fake physical addresses and easily-obtained anonymous email accounts, we have found it more or less hopeless to expect bad actors not to easily regain access to any marketplace from which they were ejected. Payment and banking information would potentially be the best route to find these actors. Unfortunately, tracing such information is beyond the current proficiency of this games publisher; and e-commerce platforms have thus far been unwilling to provide us with much detail on the financial transactions of bad actors.

After Asmodee proved a large e-commerce platform had procured and sold counterfeit goods *on its own account,* we did not see a rush to account ability, a willingness to enact realistic compensation for the damage wrought, or even a *mea culpa,* from the platform operator.

Legal routes in pursuing these matters against e-commerce platforms are not attractive due to: (a) the size of these organizations and the proportional cost of legal action; (b) the economic necessity to continue selling our products to these platforms; and (c) DMCA-related legal precedents based on a few cases brought by small, poorly funded, plaintiffs.

We maintain a consistent vigil against counterfeiters. This requires ongoing communication with our trade customers, continuous oversight of consumer reports and reviews, and a never-ending search across active e-commerce offers worldwide. We provide our customers with swift notice to share any clear evidence of counterfeiting, in order to seek removal of the suspected counterfeit distributors from their platform. We constantly employ exhaustive and expensive manual and automated policing assistance to take down sites operated by counterfeiters from within, and outside of, our distribution network. This feels like a never-ending battle.

16. If you become aware of a counterfeit good and/or distributor on your platform, what actions including initiating legal action does your company have the power to take?

Asmodee does not operate an Internet platform.

With regards to our customers' e-commerce platforms, we seek removal of the offending counterfeit goods and/or counterfeiter. Should a trade customer fail to act appropriately, we may curtail or terminate our business with that customer. We may even seek recourse through the judicial system, but this faces the issues raised in point 15 above.

17. How have you coordinated with U.S. federal and local authorities to curtail the distribution and manufacture of counterfeit goods within the United States?

Wherever possible, we provide the USCBP with product and brand registration material, guides, and other information to help facilitate the identification and seizure of counterfeit products. This is an ongoing process for Asmodee. Where the authorities allow, we do the same in other select countries.

To date, we have tried to work primarily with our e-commerce platform customers by assisting with counterfeit detection and prevention. This engagement has been *far* from mutual and remains very one-sided in favor of the e-commerce platforms.

We have worked off and on with an e-commerce platform to identify a counterfeit distributor and to refer this counterfeiter to the Office of Homeland Security. Even in this, however, the e-commerce platform has shared very little data, so Asmodee has been a follower rather than a partner in this process.

As many of the counterfeit sellers are either impossible to track, or originate outside of the U.S., we have limited ability to provide federal or local authorities with viable targets.

18. If there are other pieces of information, details, or data you feel would be helpful to the committee, we respectfully request that you submit them as part of your answers as well.

E-commerce enabled counterfeiting has become a huge problem for intellectual property holders, brick-and-mortar retailers, and to consumers. To Asmodee and our industry, it is an existential issue. Supported by modern technology, the prevalence of online anonymity, and lack of accountability for their chosen e-commerce sales platforms, operators who would previously sell their counterfeit goods on the street and in dark alleyways, have unprecedented and direct access to their marks. Given the sophistication, investment, and scale of the counterfeit operations, one comes to suspect these efforts may be managed by well-funded criminal organizations.

In our view, the facilitating factors in the deluge of counterfeit product on e-commerce platforms are:

(1) *Supply:* Countries with low-cost but robust manufacturing sectors, combined with weak internal IP enforcement, have economic benefit in overlooking the substantiality of their counterfeit exports. China surely is the largest contributor to the problem, but illicit manufacturing will likely change to other countries if China was to remedy its significant shortfalls in this area.

As this memo is written, the U.S. looks to impose new tariffs on goods originating in China. While such trade measures may be necessary (this being beyond our expertise to determine), we believe a focus on legislation and action that forcefully targets online counterfeiting would have a substantial and positive impact on the U.S. trade imbalance with China. We recommend such measures be fast-tracked. Further, such action will likely be positively supported by our European allies, who are afflicted by similar (if not as severe) counterfeiting problems.

(2) *Legislation:* The DMCA Fair Harbor standards for online platforms was intended to protect the nascent Internet. The resulting commercialization of the Internet has evolved into handful of dominant Internet business behemoths exploiting a vacuum of accountability while profiting from illicit transactions and traffic on their platforms.

New or revised legislation is critically needed to address this issue. Asmodee provides a few recommendations for specific solutions at the end of this document.

(3) *E-commerce Platforms:* Unlike their public statements, expressions of support, P.R. efforts and platitudes to the problem, it is our firsthand experience that major e-commerce platform businesses fall *far* short in taking responsibility and action in this area. The practical capabilities of so-called "sophisticated platform software" such as "Brand Registry" is poor, its use solely reactionary (not preventative), with highly disproportional burdens of proof on the rights-holders.

It is our opinion that current efforts in counterfeit prevention by e-commerce platforms is window-dressing enacted to meet whichever minimum legal and P.R. standards are necessary for them to continue business-as-usual. We do not see obvious public statements such as "Zero Tolerance for Counterfeits" in practice. We come to this opinion from experience

Asmodee has been continually turned down in data-requests to e-commerce platforms related to sales and supply of our own products, information that would allow us to assist the platforms with detection of counterfeiting activity. Instead, only an extremely limited data-set is ever shared with us, and this only after ANA proves a product to be counterfeit—usually after procuring a sample ourselves by purchase on the e-commerce platform itself. In many cases, once we have gone through with this exercise, substantial damage has already been done.

Most e-commerce platforms refuse to adhere to any form of sales policy or "authorized reseller" program (by which companies like Asmodee could contribute to the anti-counterfeiting effort and help guarantee authenticity). We have proof that a large e-commerce platform procured counterfeit products to sell on its own account, knowingly or unknowingly, by utilizing automated, algorithmic purchasing systems that search for the lowest available price, and with little/no human oversight. Some platforms sell counterfeit products on their own account from "co-mingled" product assortments—behavior that may also incriminate and destroy the reputation of honest sellers on the platform, whenever the e-commerce platform operator fulfills such sales with counterfeits tainting "co-mingled" inventories.

(4) *Consumers:* Consumers have, for good reason, learned to trust the commercial U.S. retail system. Consumers are both trusting and price-sensitive, making them ideal targets for low-priced counterfeit products sold under the trusted aegis of large U.S. e-commerce platform retailers.

Despite recent government investigators finding that 20 out of 46 randomly purchased items on a sampling of e-commerce platforms being counterfeits, despite hundreds of thousands of dangerous counterfeit solar eclipse glasses sold online, despite dangerous counterfeit cosmetics and hygiene products, counterfeit vitamins, counterfeit pet-medicine, despite the myriad stories of honest businesses injured by counterfeiting, consumers unfortunately have a convenience and financial incentive to ignore the problem or dismiss such information.

It clearly is in the e-commerce platform's best interest to perpetuate the consumer's false sense of safety. Outside small print, no clear warning regarding potential counterfeit products on e-commerce sites exist to our knowledge. Reviews that profess to counterfeits may be struck and obfuscated by the e-commerce platforms by editorial such as "This item was fulfilled by [Platform], and we take responsibility for this fulfillment experience."

(5) *Mail Subsidy:* It is our understanding that the United Nations (via the Universal Postal Union), partly with U.S. help, subsidize developing nation's mail and package delivery cost via uneven application of "Terminal Dues," effectively making it much cheaper to post mail from these developing nations. As such, the cost of sending a package from China to the U.S. is very small. This greatly facilitates not only counterfeit trade (financially transacted by U.S. e-commerce platforms) into the U.S., but also assists in illegal shipments of drugs and other contraband.

We are happy to offer specific case histories, material, or evidence that might be helpful to the committee as it seeks to protect the U.S. consumer in this ongoing struggle against the circulation and sale of counterfeits in e-commerce.

Recommendations

We believe the following actions would solve many of the current counterfeiting problems (as well as perhaps the malign "fake ads" problem) on the Internet.

(1) No product (or message) should be sold by an Internet platform into the U.S. without a U.S. person or entity being accountable for the product or message.

Those Internet platforms that allow third-party sales of products or messages should be responsible to ensure that a real U.S. person or U.S. entity is accountable for the safety, legality, and authenticity of their message or product. If it is later found that a selling person or entity was itself "fake," or if the selling entity is non-U.S., the Internet platform would then be held accountable for the sale, with whatever civil or criminal penalties apply.

(2) Grant IP holders substantially more authority to access data from Internet platforms (including e-commerce platforms) related to the commercial exploitation of their IP-related products or services offered on the platform. For example, if a counterfeit product has been proven to be sold by an e-commerce platform, the IP-holder should have the right to access comprehensive sales and supply information from all vendors and sellers whom have transacted in that IP during the last 12 months, so that IP-holders may help prevent future abuse and identify potential theretofore unknown abuses. Further, e-commerce platforms should be required to disclose known counterfeiting to rights holders and affected consumers.

(3) Many e-commerce platforms transact business alongside their platform participants (*i.e.,* third-party sellers). This behavior is tantamount to having your

cake and eating it too, and inherently unfair competition to the other platform participants. Any Internet platform that partakes directly in income-generating activity alongside the users of its own platform should be prevented from seeking Fair Harbor protection under the DMCA (or whatever will replace the existing DMCA).

(4) Internet platforms should not be allowed to physically "co-mingle" products from different marketplace sellers (and their own goods). If the platform elects to do so, it should be accountable for any sale of a counterfeit good from the tainted supply source. This accountability should be retroactive to the passage of the DMCA (October 12, 1998), and e-commerce platforms should remediate vendors, sellers, and consumers for damage done in the intervening years.

(5) Eliminate all subsidies on posted mail and packages from China immediately and as soon as practicable, abolish the program altogether lest the issue be transferred to other nations. With today's email and Internet access this program seems outdated, and subsidies for developing nations are likely better granted in alternate ways (such as providing them Internet access).

In Closing

Please feel free to contact us directly with any further questions, concerns, or requests. We intend to provide the committee with whatever assistance we can offer. This is of the highest priority to us.

Asmodee wishes the committee good luck in its effort to better inform American consumers of the dangers presented by counterfeit goods, and to better protect American consumers and businesses in the future. Thank you for working on behalf of our company, our team, our consumer community, and our nation.

Respectfully yours,

Christian T. Petersen
CEO
Asmodee North America, Inc.

Pete Fenlon
CEO
Catan Studio (an Asmodee Division)

COALITION TO COMBAT COUNTERFEITING (CCC)
10340 Democracy Lane, Suite 204
Fairfax, VA 22030
P: (703) 383–1330
F: (703) 383–1332
E: MMoonier@mwcapitol.com

Written Testimony of Mitchell Moonier

Chairman Hatch and Members of the Committee,

My name is Mitchell Moonier, and I am submitting testimony on behalf of the Coalition to Combat Counterfeiting (CCC)—a national anti-counterfeiting coalition representing a broad spectrum of industries including apparel and footwear, special occasion dresses, home appliances, jewelry, precious metals, and toys. Our mission is to raise public awareness of counterfeiting, and to support public policies, regulations, and innovative solutions for strengthening the ability to identify fake goods and enforce intellectual property rights (IPR).

Background

The expansion of e-commerce has given domestic manufacturers greater access to consumers across the globe and has lowered costs for doing business. Likewise, it has also enhanced the ability for fake goods to enter the market and successfully compete with their legitimate counterparts. Many of these fakes pose numerous health and safety risks to American families, steal domestic jobs, and defraud the economy. Before, counterfeit products were confined to small street operations with limited reach, but the growth of e-commerce has allowed these hazardous fakes to surround our daily lives. Every day, we hear of consumers encountering everything from coats stuffed with chicken feces, water filters that filter arsenic into the water rather than remove it, and children's toys that fail to meet even the slightest of safety standards.

Businesses—both large and small—lose out, as well. Instead of researching and developing new innovative products, more funds are redirected to counterfeit deterrence programs. A recent report by the U.S. Chamber of Commerce found companies spending as much as $20 million annually to protect intellectual property. For smaller "mom and pop" shops unable to afford such protections, it is better to lower

prices than compete with the inferior goods. The costs add up—recent estimates show that the U.S. economy loses anywhere from $225 to $600 billion a year.

The impact on business, large and small, of consumption of counterfeits is that production shifts from legitimate businesses to shady manufacturers. In addition to operating under inhumane conditions, these operations in many cases are connected to terrorism, money laundering, and human trafficking.

The work of Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) is vital for protecting American IPR. Over the past decade, seizures of fake goods have increased 117 percent and the total retail price of seizures increased 800 percent. These statistics illustrate the significance of the problem and that it is growing worse. The $1.6 billion in seized goods for 2016, based on conservative estimates, represents less than 1 percent of the total estimated amount of fake goods that entered our borders. Counterfeiters are targeting higher value products and the U.S. economy is losing at a faster pace. Customs agencies are more technologically advanced than ever before, yet counterfeiters, in response, have shifted to simpler methods to evade detection by the authorities including using express carriers and international mail.

We realize that there is not a "one size fits all" solution that fully addresses the counterfeiting of goods. The growth of e-commerce has rapidly outpaced innovation in protecting intellectual property, and improvements are needed before it becomes too late. It goes without saying that such an endeavor will require significant time and funding, but we believe both are necessary as this issue is an ongoing threat to our national security.

Recommendations

The findings from the recent GAO report should be concerning to rights holders and consumers alike. In addition to the act of counterfeiting, itself, issues with data collection and information sharing among enforcement agencies threaten the preservation of intellectual property. Moving forward, we share many of GAO's concerns and believe that the following recommendations would significantly improve enforcement against counterfeit goods.

Improve International Cooperation

Greater cooperation is needed between U.S. and international customs authorities. In a report released last week, the Organization for Economic Cooperation and Development (OECD) estimated that 2.5 percent of global trade, or $461 billion, consists of fake goods. Furthermore, 20 percent of global intellectual property infringements are of U.S. rights holders. Our participation in the global economy means that U.S. intellectual property must be protected both at home and abroad, alongside our international partners. On the other hand, consequences should be strongly considered for trading partners that lack adequate laws or enforcement of U.S. intellectual property.

Assess Interagency Efforts

There needs to be a broader assessment of CBP interaction with other domestic agencies. Agencies including the United States Patent and Trademark Office (USPTO), Department of Commerce, United States Trade Representative (USTR), United States Postal Service (USPS), and the Federal Bureau of Investigation (FBI) also play an important role in protecting intellectual property. However, each agency employs its own recording methods for seized goods and may share limited information with CBP. This makes it difficult and confusing for rights holders to protect their intellectual property, and effectively engage with law enforcement.

We support further assessments by the GAO that evaluate the sufficiency of current laws in protecting intellectual property, the extent in which all IP-related agencies coordinate with each other, and each agency's metrics for evaluating intellectual property protection.

Express Carriers and International Mail

The use of express carriers and international mail should be a focal point in the fight against counterfeits. Since 2012, seizures of express carrier goods have increased 105 percent while cargo seizures have only increase 6 percent. The volume of small packages makes it impossible for customs authorities to detect infringing goods, and the problem is further complicated with the use of fake labels that often assist in evading customs duties.

Increase Engagement With the Private Sector

We support the GAO's recommendation for CBP to share additional information with intellectual property rights holders prior to completing a seizure, as authorized under the Trade Facilitation and Trade Enforcement Act (TFTEA). Although CBP received authorization almost three years ago, the GAO notes that it has yet to determine which information would be beneficial to share with the private sector. It is important that CBP make these determinations immediately, so rights holders can act appropriately. Additionally, the government should explore public-private partnerships to strengthen detection and enforcement efforts, particularly to address the issue of small package shipments through express carriers and international mail.

While we have identified multiple areas of improvement in the national intellectual property enforcement framework, we applaud the attention given to these issues by Congress and the appropriate agencies. We look forward to continuing to work together to protect U.S. intellectual property rights and consumers from these harmful products.

The Coalition appreciates the opportunity to submit these comments to the Committee. Should you or your staff have any questions, please feel free to reach out to us. We are more than happy to meet with you or your staff to discuss these critical issues impacting our businesses and consumers.

THE COUNTERFEIT REPORT
P.O. Box 3193
Camarillo, CA 93010
(805) 303–5000

Statement of Craig M. Crosby Publisher/CEO

Senator Hatch, I would like to thank you for your interest in consumer protection from counterfeit products, and inviting statements from those in the industry affected by counterfeits.

I am the CEO and Publisher of *The Counterfeit Report®*, a consumer protection advocate and industry watchdog reaching over *7.5 million viewers* that has removed over *26 million* counterfeit products from e-commerce websites including eBay, Amazon, Walmart and Alibaba.

These websites are the ideal platforms for enabling and facilitating counterfeiters and dishonest sellers to distribute an inexhaustible supply counterfeit goods directly to unsuspecting consumers with little or no consequence to the seller or e-commerce websites.

Counterfeiters will produce over **$1.7 trillion** in counterfeit products[1] in 2018, 90% of which originate in China. An overwhelming majority are distributed through e-commerce websites.

The Counterfeit Report ("TCR") research has been cited, and TCR deposed, in the federal court RICO lawsuit against eBay (*Wimo Labs, LLC v. eBay* 8:15–cv–01330), which settled and was sealed in 2017, and the pending landmark Amazon (as a direct seller) lawsuit (*Daimler AG v. Amazon,* U.S. District Court 17–cv–7674).

Clearly, these goliaths facilitate criminal activity and benefit from the proceeds of dishonest actions which impact jobs, consumer safety, and public trust, creating a public perception of deception with impunity.

TCR purchased **over 2,500 manufacturer confirmed counterfeit products** from eBay, Amazon and Walmart sellers, representing over **726,400 fakes sold** to duped consumers. Each counterfeit purchase is cataloged and retained as evidence, identifying the seller, point of origin, and number of items sold, as well as dozens of other data points.

Please note that **Alibaba** is not specifically addressed here, as Alibaba has been publicly condemned by The Office of the United States Trade Representative and placed on the *U.S. Notorious Markets List*—a designation reserved for the world's most notorious markets for counterfeit goods.

---

[1] "The Economic Costs of Counterfeiting and Piracy." The report was prepared for The International Chamber of Commerce Business Action to Stop Counterfeiting and Piracy unit (ICC BASCAP) and The International Trademark Association (INTA), January 2017, Frontier Economics, Ltd.

Industry research indicates that 80% of consumers do not expect to receive a counterfeit when making online purchases, yet over one-third of consumers unwillingly received a fake[2] from online purchases last year. The purchases include dangerous and deadly counterfeit products, and inarguably fake items such as FBI and police badges, and law enforcement ID.

For example: Counterfeit Apple® A1265 iPhone chargers are common on eBay and Amazon. Counterfeit chargers have caused two deaths, one coma, numerous fires, and injuries from explosions and equipment damage. Just two of the many eBay sellers selected by *The Counterfeit Report* for test purchases made over 10,000 sales of confirmed counterfeit chargers to unsuspecting consumers, yet the listings and sellers remained. The buyers were never notified by the websites. Test purchases also include auto suspension parts, OTC drugs, medical devices, toys, electronics, health supplements, and much, much more.

The Counterfeit Report investigation uncovered that eBay and Amazon deliberately and fraudulently hide the fact from buyers that they have purchased manufacturer confirmed counterfeits and are entitled to refunds. But, buyers are never told this—in fact, eBay tells buyers opposite in their eBay purchase history for removed counterfeit listings "the sale should process as normal and you have nothing to worry about."

You would be shocked to learn that the e-commerce giants **solicit, facilitate, and encourage** the sale of hundreds of millions of Counterfeit Products through their self-described "ecosystems," which provide manufacturers, sellers, and buyers of counterfeit goods a marketplace for such goods, and provide online advertising, marketing, credit card processing, financing, and shipping services that effectuate the sale of the Counterfeit Products. Of course, they take a transaction fee for each fake item sold.

Amazon and Walmart also act as direct sellers of counterfeits, in addition to allowing unvetted global third-party "marketplace" sellers to list just about anything on their websites, including counterfeits, right alongside authentic items, implying the websites endorsement.

I have appeared on ABC, NBC, FOX, 20/20 and other TV network presentations featuring counterfeit products. TCR distributes counterfeit information to over 2,000 news outlets. I have presented for the LAPD, LA City Attorney, and the FBI in a fake goods news conferences.

The Counterfeit Report website provides consumer education, featuring visual guides to counterfeit products of over 250 global manufacturers. TCR also acts as an authorized agent for right holder's infringing products, and publishes individual *Counterfeit Product Alerts®* on counterfeited product on its website. The alerts offer thousands of comparison photos demonstrating the sophistication of counterfeiters in creating deceptive, visually identical counterfeit products that easily fool consumers. Quite simply, most consumers simply can't identify counterfeit products and are unknowing victims who lose billions of dollars and may receive a deadly product.

What I think may interest you most is the outrageous conduct of the internet giants, eBay, Amazon and Walmart. TCR test purchases identified and documented practices, policies and procedures that satisfy the **ongoing** pattern of criminal conduct; fraud, false advertising, unfair business practices, Racketeering (RICO), and conduct that is not consistent with ordinary business conduct and an ordinary business purpose to provide consumers with honest services (18 U.S.C. § 1346). For example:

- Amazon, eBay, Walmart and Alibaba all have policies prohibiting *replicas, fakes, counterfeits, or other illegal copies on their websites. However, that claim is not true.* A TCR Press Release identifying the particularly alarming sale of inarguably fake FBI and Police badges and made-to-order photo identification on eBay was emailed to eBay CEO, Devin Wenig. The email was viewed 304 times, yet over a year later, the eBay listings remain. Similar results occurred with Amazon, also selling the fake law enforcement items.
- A consumer would expect to be notified they have purchased a dangerous, fraudulent or deadly product on eBay, Amazon or Walmart, and are entitled to a refund under the *Money Back Guarantee* displayed on each website's listing page. However, in practice, a buyer viewing their eBay purchase history

[2] "Global Online Shopping Survey 2017—Consumer Goods." Prepared by: Clarivate Analytics for MarkMonitor® Inc., November 2017.

after a counterfeit listing is removed is deliberately misled with the message "If you've already sent payment, the sale should process as normal and you don't have anything to worry about." The opposite may be true, and buyers could have a lot to worry about if they received a dangerous product. Amazon does not post any warning.

- Buyers that actually do identify a counterfeit item can request a refund under eBay's *Money Back Guarantee,* but there is a catch: eBay directs buyers to return the item to the seller, a nonsensical solution promoting resale; against eBay policy and illegal. If challenged, eBay requires a manufacturer's written counterfeit confirmation, allowing buyers just **2 to 5 days,** and arbitrarily requires that "in order to continue with the investigation of your Money Back Guarantee, you must destroy and discard the item." Clever, but without the counterfeit item, buyers have no evidence for their unresolved eBay claim, credit card refund or counterfeit feedback.

eBay went as far as to engage two goliath international law firms, Winston and Strawn and O'Melveny and Meyers, in an attempt to silence *The Counterfeit Report's* findings. Using scorched earth litigation tactics for two arbitrations initiated by *The Counterfeit Report* for refunds of inarguably fake $26 and $116 item purchases, eBay's attempt to dissuade *The Counterfeit Report* failed. I am happy to share with you all the correspondence and court documents.

eBay and Amazon "User Feedback" should provide valuable insight to the Buyers and Sellers involved in a transaction—allowing each to build reputations that are based on ratings and comments left by their trading partners—but it doesn't.

- Inexplicably, negative "counterfeit" feedback left to protect eBay and Amazon consumers from dishonest seller practices just "disappeared" after many of the confirmed counterfeit purchases by *The Counterfeit Report.* eBay's leadership team had no explanation why the "in policy" feedback was removed, while Senior Director and eBay Counsel, Amber Leavitt, acknowledged, but never responded to *The Counterfeit Report's* inquiry.
- Under eBay policy, "Sellers *can leave only positive ratings* for buyers. That means buyers should feel free to leave honest feedback without fear of retaliation."
- eBay blocks buyers from placing seller feedback, removes negative seller feedback, and arbitrarily removes links for buyers to provide seller feedback for known manufacturer confirmed counterfeit and fake products. In 2015, eBay admitted the allegations were true to *Business Insider,* that **eBay** altered and removed feedback, removed warnings, and allowed counterfeit sellers to remain. Amazon blocks negative counterfeit feedback.

eBay and Amazon marketing and support practices encourage the sale of counterfeits.

- Through manipulation of its "keyword" search process, consumers searching Amazon, eBay and Walmart for a trademarked item are guided to listings of known, manufacturer confirmed counterfeit and fake products.
- Amazon cancelled all TCR refunds for confirmed counterfeit product purchases, later rescinding the action after a press release.
- eBay chose to block TCR test purchases, and disclosed to sellers effective ways to block TCR test purchases of counterfeit and fake items, identifying the multiple accounts used by TCR. This policy is endorsed by eBay's Director of Global Trust Policy, Gary Fullmer, with his written warning to *The Counterfeit Report,* "Do not circumvent these blocks, including using your multiple accounts to do so."
- Remarkably, eBay sends direct email solicitations to consumers (over 4,000 just to TCR) to purchase the fake items—a practice that landed eBay in Federal Court—yet the practice continues and the counterfeit sellers remain.

eBay claims it's "just a venue" and has immunity under eBay's often cited 2008 *Tiffany (NJ) Inc. v. eBay Inc.* lawsuit.

- However, eBay allows staffers to determine if items are accurately described in counterfeit purchase dispute cases despite the manufacturer's written counterfeit confirmations—an action that landed eBay in arbitration in which *The Counterfeit Report* prevailed.

- Despite repeated written notifications to Amazon, eBay and Walmart of the sale of the same manufacturer confirmed counterfeit, and fake products—products that never existed in the authentic product line but bear a trademark—the items and sellers often remain, and additional purchases have been made from over a period of months.
- While Amazon was publicly initiating lawsuits against two Amazon counterfeit sellers, sharply contrasting activity was occurring in the background. Amazon argued and won a U.S. Appeal's Court decision[3,4] to disavow itself from any responsibility for "offering to sell" counterfeits products. Shortly thereafter, a lawsuit named Amazon a direct seller of counterfeits, outside the protection of the prior decision.

I hope you agree that the abundance of evidence is compelling and worthy of a continued investigation.

PRECIOUS METALS ASSOCIATION OF NORTH AMERICA
10340 Democracy Lane, Suite 204
Fairfax, VA 22030
P: (703) 383–1330
F: (703) 383–1332
E: Mail@mwcapitol.com

Written Testimony of Scott Smith, President

Chairman Hatch and Members of the Committee,

My name is Scott Smith, and I am the CEO of Pyromet, which is a privately owned precious metals manufacturer and refiner of silver, gold, and platinum group metals. Since 1969, Pyromet has been a reputable name in precious metals and precious metals management. I also serve as President of the Precious Metals Association of North America (PMANA) and am submitting this written testimony on behalf of our members. It is our traders, distributors, and authorized purchasers of the United States Mint that are particularly concerned with counterfeit bullion produced in the People's Republic of China, and subsequently sold on e-commerce platforms.

Background

According to the Organization for Economic Cooperation and Development (OECD), the trade of fake goods represents 2.5 percent of global trade, or $461 billion every year. Among the many counterfeits traded globally each year are fake precious metals bullion coins and bars—most of which are produced in China and easily distributed through e-commerce platforms. Additionally, estimates show over 85 percent of U.S. counterfeit goods originate in China.

Precious metals bullion has been introduced by numerous national governments and private mints around the world for nearly fifty years. The U.S. began production of its own bullion in 1986 with the introduction of the American Eagle Gold coin. Since then, the American Eagle family has since expanded to include silver, platinum, and palladium bullion coins.

U.S. Mint bullion coins are not sold directly to the public. Instead, authorized purchasers that satisfy stringent financial and professional criteria buy bullion coins and sell them at a premium to investors. Precious metals bullion can also take the form of bars—or ingots—and are usually produced by private mints from around the world and are sold by domestic traders and distributors. This network of bullion distributors, many of whom are members of the PMANA, includes some of the most trusted names in the precious metals industry. When investors are deceived by counterfeit bullion, distributors' brands, and jobs all along the precious metals supply chain, are significantly affected.

Whether in coin or bar form, it is relatively easy to pass off counterfeit bullion as authentic. Manufacturers will often coat, or "plate," tungsten in a thin layer of gold. Since tungsten and gold have nearly the same weight and density, plated coins can

---

[3] In a devastating blow to manufacturers and consumer protection, the U.S. Court of Appeals upheld a U.S. District Court decision by Judge Ricardo S. Martinez excusing Amazon (NASDAQ: AMZN) from liability in the sale of counterfeit items on its website (*Milo & Gabby, LLC. v. Amazon.com, Inc.*).

[4] Wade Shepard, "As Amazon and eBay Flood With Illegal Goods From China, Beijing Cracks Down on Foreign E-Commerce," *Forbes* (November 22, 2017), available at: *https://www.forbes.com/sites/wadeshepard/2017/11/22/as-amazon-and-ebay-flood-with-illegal-goods-from-china-beijing-cracks-down-on-foreign-e-commerce/#7223fl604dfd.*

pass a novice investor's basic tests. Even the most experienced precious metals traders require spending as much as $100,000 on innovative technology to detect fake bullion. At the time of submission, one-ounce of gold is worth $1,322, but a gold-plated one-ounce counterfeit coin or bar can be purchased from a Chinese manufacturer for as low as $250—a potential 427% return on investment for criminals. While criminals profit, our traders and distributors are affected with damaged brands, falling revenues, and less capital to purchase additional bullion for investors. Furthermore, the decrease in demand for bullion causes refiners and manufacturers along the supply chain to suffer.

The problem has grown in recent years with the explosion of e-commerce trading and its ability to connect consumers to the worldwide market. At the same time, it has also given Chinese manufacturers, with the backing of their government, greater access for selling fake goods.

Chinese law requires truth in advertising, which also means that counterfeit bullion products be sold as such. However, the law does not require that counterfeits be physically marked accordingly. With this legal shortcoming, e-commerce sites such as Alibaba are flooded with posts that advertise counterfeit bullion as "replica," "copy," and "fake." While this is completely legal in the People's Republic of China, it gives government-sanctioned manufacturers the ability to manipulate vulnerable American consumers and those looking to defraud consumers in the future. In other words, if they are not deceiving American consumers directly, they are providing domestic criminals with the necessary tools to do so in the future. On their web profiles, Chinese manufacturers often tout the ability of their counterfeit bullion to pass as the real thing. Answers to "frequently asked questions" make potential buyers aware that counterfeit coins are non-magnetic, weigh almost identical to authentic coins, and pass most authentication tests. Clearly, their intent is to deceive consumers in one way or another.

Further complicating customs authorities' ability to track fake bullion, thieves use small packages, fake labels, and ship through express and international mail to evade detection and the payment of duties. Over 90% of goods seized by Customs and Border Protection (CBP) come through either express or international mail. While this statistic is encouraging, we know that far too many small packages successfully pass-through customs to their targeted destination.

Policy Proposal

In order to combat the spread of counterfeit coins through e-commerce networks, and to lessen the already significant burden placed on law enforcement, the PMANA urges Congress to amend 15 U.S. Code § 2101 to expand marking requirements to include bullion investment coins and bars. Doing so would require any imitation or replica item manufactured or imported into the United States to be plainly and permanently marked "Copy" or "Replica." This would provide transparency for consumers and weaken the ability for domestic and international criminals to take advantage of them.

Additionally, the PMANA urges the United States Trade Representative (USTR) to include language in future trade agreements that holds all parties to the same marking requirements as U.S. citizens under 15 U.S. Code § 2101, as amended with language relating to investment bullion. This trade provision would generate jobs along the precious metals supply chain, protect consumers, and generate tax revenue in both counterfeit producing countries and in the U.S.

Thank you for giving the PMANA the opportunity to submit these comments to the Committee. If you or your staff have any questions, please do not hesitate to reach out to us. We are more than happy to discuss our concerns with you or your staff and look forward to working together to protect consumers and businesses from counterfeit products.

Respectfully Submitted,

Scott Smith

○