IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HONG KONG LEYUZHEN TECHNOLOGY CO. LIMITED, Plaintiff, v. Shenzhen Yilanya Technology Co., Ltd., Defendants.	**Case No.: 1:25-cv-04947-MMP-HKM** **Honorable Martha M. Pacold** **Magistrate Heather K. McShain**

PLAINTIFF'S RENEWED *EX PARTE* MOTION FOR ENTRY OF A TEMPORARY RESTRAINING ORDER

Plaintiff Hong Kong Leyuzhen Technology Co. Limited, ("Plaintiff"), by and through its counsel, the Bayramoglu Law Offices, LLC, hereby moves for this Court for Entry of a Temporary Restraining Order, including a temporary injunction and expedited discovery, (the "Motion"). Plaintiff files herewith a Memorandum of Law in support, the Declaration of Katherine M. Kuhn, the Declaration of Liangjie Li and accompanying exhibits.

DATED: July 3, 2025

Respectfully submitted,

By: */s/ Katherine M. Kuhn*
Katherine M. Kuhn (Bar No. 6331405)
BAYRAMOGLU LAW OFFICES LLC
233 S. Wacker Drive, 44th Floor, #57
Chicago, IL 60606
Tel: (702) 462-5973 Fax: (702) 553-3404
Katherine@bayramoglu-legal.com
Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on the 3rd day of July 2025, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Northern District of Illinois, Eastern Division, using the electronic case filing system. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

Respectfully submitted,

By: */s/ Katherine M. Kuhn*
Katherine M. Kuhn (Bar No. 6331405)
BAYRAMOGLU LAW OFFICES LLC
233 S. Wacker Drive, 44th Floor, #57
Chicago, IL 60606
Tel: (702) 462-5973 Fax: (702) 553-3404
Katherine@bayramoglu-legal.com
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HONG KONG LEYUZHEN TECHNOLOGY CO. LIMITED, Plaintiff, v. Shenzhen Yilanya Technology Co., Ltd., Defendants.	**Case No.: 1:25-cv-04947-MMP-HKM** **Honorable Martha M. Pacold** **Magistrate Heather K. McShain**

MEMORANDUM IN SUPPORT OF PLAINTIFF'S RENEWED *EX PARTE* MOTION FOR ENTRY OF A TEMPORARY RESTRAINING ORDER AND EXPEDITED DISCOVERY

I. INTRODUCTION AND SUMMARY OF ARGUMENT

Plaintiff has filed this copyright infringement action against the Defendant, Shenzhen Yilanya Technology Co., Ltd., for Defendant's unauthorized use and reproduction of Plaintiff's Copyright-Protected Images. Plaintiff seeks temporary *ex parte* relief based on this action filed against Defendant alleging two causes of action; Count I - Copyright Infringement and Count II- Violation of the Illinois Uniform Deceptive Trade Practices Act.

As alleged in Plaintiff's Complaint, Defendant is publicly displaying unauthorized and unlicensed reproductions of Plaintiff's Copyright-Protected Images, specifically, images from Plaintiff's 2022 Swimwear Collection. Defendant's unauthorized use of Plaintiff's Copyright-Protected Images, covered by valid U.S. copyright registration VA0002379888, is a deliberate appropriation of these precise swimsuits from Plaintiff's 2022 fashion trend collections. Defendant markets, sells, and distributes competing products by using unauthorized and unlicensed

reproductions of Plaintiff's Copyright-Protected Images through various fully interactive and commercial Internet stores operating on the Alibaba.com Online Marketplace Platform.

Defendant in this action runs a sophisticated online operation by running one or more interactive and commercial Internet stores functioning on the Alibaba.com Online Marketplace Platform. Through these online stores Illinois residents can view the unauthorized and unlicensed reproduced images of Plaintiff's lawfully Copyrighted-Protected Images on these infringing Internet Stores and then make purchases of the competing products unaware the true origin of the product. Moreover, Defendants attempt to avoid liability by going to great lengths to conceal both their identities and the full scope and interworking of their operation. Therefore, Plaintiff is forced to file this action to combat Defendant's continued infringement of its copyrights, as well as to protect unknowing consumers from purchasing competing products over the Internet without knowing the true origin of the product. Defendant's ongoing unlawful activities should be restrained. As of the date of this filing, the link identified in Plaintiff's First Amended Complaint is still active and displaying Plaintiff's Copyright Protected Images [Dkt. No. 22-5], and Plaintiff respectfully requests that this Court issue an *ex parte* Temporary Restraining Order against Defendant, Shenzhen Yilanya Technology Co., Ltd.

II. STATEMENT OF FACTS

A. Plaintiff's Products and Copyright

Plaintiff designs, manufactures, sells, and distributes a wide variety of products including Women's clothing and apparel (collectively, "Plaintiff's Products"). (See Declaration of Liangjie Li., filed concurrently herewith (the "Li Decl.") ¶ 7.) Plaintiff generates approximately $20,000,000 in revenue, and well over $1,000,000 derived from the State of Illinois, from sales of its products through its website, rotita.com. Plaintiff does not sell or offer or authorize the sale of

its merchandise on any other online platform, such as Amazon, eBay®, Aliexpress, Alibaba, Walmart, or TikTok, and several other online and offline stores. (Li Decl. ¶ 8). Plaintiff incorporates a variety of Copyright-Protected Images stemming from Plaintiff's original authorship of the fashion trend collections and the products associated with each collection. (Li Decl. ¶ 10). Here, Defendant has deliberately infringed on Plaintiff's U.S. Copyright-Protected Images containing the following Copyright Registration Number VA0002379888, (the "Asserted Copyright"). Plaintiff is the lawful assignee of all right, title, and interests in the Asserted Copyright. (Li Decl. ¶ 12).

The Asserted Copyright and its registrations have been duly and legally issued by the United States Copyright Office. (See Exhibit 1 to the First Amended Complaint). The Asserted Copyright is currently unexpired, valid, and enforceable. Plaintiff has not granted Defendant any license under the Asserted Copyright. (Id. ¶ 7). Plaintiff has registered several of its Copyright-Protected Images with the United States Copyright Office. (Li Decl. ¶ 6). The exclusive rights granted to Plaintiff under the U.S. Copyright Act for its Copyright-Protected Images include the exclusive right to reproduce, publicly display, and distribute Plaintiff's Copyright-Protected Images to the public. Plaintiff uses its Copyright-Protected Images extensively in connection with the marketing of Plaintiff's Products. (Li Decl. ¶ 14). Plaintiff has expended significant sums in advertising, promoting, and marketing Plaintiff's Products featuring Plaintiff's Copyright-Protected Images. (Id.) Plaintiff's Products embody the same photographs in the registrations of the Copyright-Protected Images. Plaintiff uses its Copyright-Protected Images exclusively in connection with the marketing of Plaintiff's Products. (Li Decl. ¶ 14). The Asserted Copyright for the Copyright-Protected Images assist in differentiating such women's clothing and apparel from those of competitors. (Li Decl. ¶ 15). Further, Plaintiff uses its Copyright-Protected Images

exclusively in connection with the marketing of Plaintiff's Products for planned fashion trend collection releases throughout each year. (Li Decl. ¶ 15). The Copyrighted-Protected Images have been highly commercially successful, with new copyright-protected images being released on a rolling cycle to keep up with changing fashion trends. *Id.* Sales of the Plaintiff's Products associated with Plaintiff's Copyright-Protected Images have generated and continue to generate substantial revenue. *Id.*

B. Defendants' Unlawful Activities

The success of Plaintiff's business and Plaintiff's Products in particular, Plaintiff's fashion trend collections has resulted in widespread infringement of Plaintiff's Copyright-Protected Images (Li Decl. ¶ 17). Consequently, Plaintiff has recently instituted a worldwide program to investigate suspicious online marketplace listings. *Id.* Defendant facilitates sales of the Infringing Products by designing their online storefronts to include unauthorized and unlicensed reproductions of Plaintiff's Copyright-Protected Images so that they appear to the unknowing consumer to be authorized online retailers, outlet stores, or wholesalers stemming from the same origin as Plaintiff's Products. Defendant's online storefronts appear sophisticated and accept payment in U.S. dollars via credit cards, Apple Pay, Western Union, and/or PayPal. (Kuhn Decl. ¶ 9). Further, Defendants often include on their online storefronts content and images that make it very difficult for consumers to distinguish such stores from an authorized retailer. *Id*. Information regarding Defendant and its infringing activity is attached as Exhibit 5 to the Kuhn Declaration ("Kuhn Decl. Exhibit 5"). This information includes Defendant's online store name, and/or sellerIDs, the URL linking to the competing product, and the unauthorized and unlicensed reproduction of Plaintiff's Copyright-Protected Images.

On information and belief, Defendant has anonymously registered and maintained aliases to prevent discovery of its true identity and the scope of its e-commerce operation. (Kuhn Decl. ¶ 11). On information and belief, Defendant has engaged in fraudulent conduct when registering its online storefronts by providing false, misleading, and/or incomplete information to multiple online platforms, including to the Alibaba Platform. *Id.* On information and belief, Defendant regularly registers or acquires new seller aliases for the purpose of offering for sale and selling infringing products on e-commerce platforms such as eBay, Amazon, Wish, Walmart, Alibaba, and temu. *Id*. On information and belief, such seller alias registration patterns are one of many common tactics used by Defendant to conceal its identity and the full scope and interworking of its operations, and to avoid being shut down. *Id*. Infringers such as Defendant commonly operate under multiple seller aliases and payment accounts so that they can continue operating in spite of enforcement efforts. (Kuhn Decl. ¶ 14). Additionally, competing products for sale by the Defendant and other Infringers' Internet Stores bear similar irregularities and indicia of being a copy of each other, suggesting that the competing and Infringing Products were manufactured by and come from the same source. (Kuhn Decl. ¶ 12).

C. Defendants Infringement Arises from Rotita's Swimwear Fashion Collections.

Here, Defendant utilizes the reputation of Plaintiff's Rotita brand ("Rotita") women's clothing to market and sell inferior, competing products by displaying Plaintiff's Copyright-Protected Images. To keep up with fashion trends and seasons each year, Rotita will publish various photos and images to advertise its collections of women's clothing to sell, including the Copyrighted works at issue in this action. (Li Decl. ¶ 19.) Upon information and belief, Defendant's display the unauthorized and unlicensed reproduced images after they are first lawfully displayed on the Plaintiff's legitimate website as part of Rotita's yearly product launches

for its fashion trend collections. *Id.* Here, Defendant in this case is alleged to be holding themself and its competing products as authentic Rotita women's clothing by confusing consumers through the unauthorized and unlicensed reproduction and public display of Plaintiff's Copyright-Protected Images. Moreover, given the nature of Plaintiff's textile manufactured women's clothing products, such large-scale sales operations over online retail platforms require considerable supply chain coordination efforts that could not reasonably be accomplished independently by Defendant. (Li Decl. ¶ 21.)

D. Jurisdiction

This Court has original subject matter jurisdiction over the claims in this action pursuant to the provisions of the Federal Copyright Act, 17 U.S.C. § 101, et seq., 28 U.S.C. § 1338(a)–(b) and 28 U.S.C. § 1331. Further, this Court may properly exercise personal jurisdiction over Defendant because Defendant directly targets business activities targeted toward consumers in the United States, including Illinois, through fully interactive and commercial online storefronts.

Specifically, Defendant has targeted sales to Illinois residents by setting up and operating e-commerce stores on Alibaba to target U.S. consumers using one or more seller aliases through which Illinois residents can purchase the competing products. Defendant has also sold and indicated that they remain ready, willing, and able to sell to residents in the State of Illinois. (Kuhn Decl., Exhibit 5) Defendant is engaging in interstate commerce, committing tortious acts in Illinois, and have wrongfully caused Plaintiff substantial injury in the State of Illinois. Venue is proper pursuant to 28 U.S.C. § 1391 and personal jurisdiction is proper as Defendant has purposely availed themselves to the laws of this jurisdiction through the direct shipment of its competing product into this jurisdiction through the use displaying and infringing upon a lawfully Copyright-Protected Image.

III. ARGUMENT

A. Legal Standard Governing Requests for a Temporary Restraining Order

A party seeking a TRO must demonstrate: (1) that its case has some likelihood of success on the merits; (2) that no adequate remedy at law exists; and (3) that it will suffer irreparable harm if the TRO is not granted. *Promatek Indus., Ltd. v. Equitrac Corp*., 300 F.3d 808, 811 (7th Cir. 2002). If the Court is satisfied that these three conditions have been met, then it must consider the harm that the non-moving party will suffer if preliminary relief is granted, balancing such harm against the irreparable harm the moving party will suffer if relief is denied. *Id*. Finally, the Court must consider the potential effect on the public interest (non-parties) in denying or granting the injunction. *Id*. The Court then weighs all these factors, "sitting as would a chancellor in equity," when it decides whether to grant the injunction. *Abbott Labs. v. Mead Johnson & Co.*, 971 F.2d 6, 11 (7th Cir. 1992). This process involves engaging in what the Seventh Circuit Court of Appeals has deemed "the sliding scale approach" – the more likely the plaintiff will succeed on the merits, the less the balance of harms need favor the plaintiff's position. *Id.* at 12.

Defendant's purposeful, intentional, and unlawful conduct is causing and will continue to cause irreparable harm to Plaintiff's reputation and goodwill. Rule 65(b) of the Federal Rules of Civil Procedure provides that the Court may issue an *ex parte* TRO where immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party or that party's attorney can be heard in opposition. Fed. R. Civ. P. 65(b). The entry of a TRO is appropriate because it would immediately stop the Defendant from benefiting from its wrongful use of Plaintiff's Copyright-Protected Images and preserve the status quo until a hearing can be held, including that as of the date of this filing, the Defendant continues to display Plaintiff's Copyright-Protected Images.

In the absence of a TRO without notice, the Defendant can and likely will register new e-commerce stores under new aliases and move any assets to offshore bank accounts outside the jurisdiction of this Court. Courts have recognized that civil actions against infringers and counterfeiters present special challenges that justify proceeding on an *ex parte* basis. See *Columbia Pictures Indus., Inc. v. Jasso*, 927 F. Supp. 1075, 1077 (N.D. Ill. 1996) (observing that "proceedings against those who deliberately traffic in infringing merchandise are often useless if notice is given to the infringers"). As such, Plaintiff respectfully requests that this Court issue the requested *ex parte* TRO.

B. Plaintiff Will Likely Succeed on the Merits

1. Copyright Infringement

Copyright infringement requires proof of "(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original." *Janky v. Lake Cnty. Convention &Visitors Bureau*, 576 F.3d 356, 361 (7th Cir. 2009) (internal citation omitted). "Because direct evidence of copying often is unavailable, copying may be inferred where the defendant had access to the copyrighted work and the accused work is substantially similar to the copyrighted work." *Atari, Inc. v. N. Am. Philips Consumer Elec. Corp*., 672 F.2d 607, 614, superseded on other grouds 722 F.3d 1089 (7th Cir. 1982). In determining whether the works are substantially similar, the Court must consider "whether the accused work is so similar to the plaintiff's work that an ordinary reasonable person would conclude that the defendant unlawfully appropriated the plaintiff's protectable expression by taking material of substance and value." *Wildlife Express Corp. v. Carol Wright Sales, Inc.,* 18 F.3d 502, 509 (7th Cir. 1994).

Plaintiff's Copyright-Protected Images are publicly available online. Defendant has, therefore, had access to these images. Further, Defendant has at least reproduced, publicly

displayed exact copies or substantially similar versions of Plaintiff's Copyright-Protected Images. See Exhibit 5 to the Kuhn Declaration for Defendant's Alibaba seller ID and infringing Product Number at issue. Based at least on the above and attached Exhibit 5 to the Kuhn Declaration, Plaintiff is likely to succeed on the merits of its claim that Defendant willfully infringes Plaintiff's copyrights covering the Copyright-Protected Images.

2. Plaintiff is Likely to Succeed on Its Illinois Uniform Deceptive Trade Practices Act Claim.

In Illinois, courts resolve unfair competition and deceptive trade practices claims, "according to the principles set forth under the Lanham Act." *Spex, Inc. v. Joy of Spex, Inc*., 847 F. Supp. 567, 579 (N.D. Ill. 1994). Illinois courts look to federal case law and apply the same analysis to state infringement claims. Id. (citation omitted). The determination as to whether there is a likelihood of confusion is similar under both the Lanham Act and the Illinois Uniform Deceptive Trade Practices Act. See *Ent. One UK Ltd. v. 2012Shiliang*, 384 F. Supp. 3d 941, 952 (N.D. Ill. 2019).

As previously demonstrated in Exhibit 5 to the Kuhn Declaration, Plaintiff has established a likelihood of success on the merits of its copyright infringement against Defendant. This standard is equally applicable under Illinois law. Accordingly, Plaintiff has established a high likelihood of success on the merits of its Illinois Uniform Deceptive Trade Practices Act claim. Accordingly, this claim, alone, satisfies the first analysis prong required to justify issuance of the requested injunctive relief.

C. There Is No Adequate Remedy at Law, and Plaintiff Will Suffer Irreparable Harm in the Absence of Preliminary and Emergency Relief.

The Seventh Circuit has held that irreparable harm is presumed in copyright infringement cases. *Atari,* 672 F.2d at 620. Indeed, in recognition of the irreparable nature of the harm caused by copyright infringement and the aim of the copyright laws to prevent such commercial harm not compensable monetarily, the Copyright Act expressly provides for injunctive relief in order to address infringement. See 17 U.S.C. § 502; *HarperCollins Publishers LLC v. Gawker Media LLC,* 721 F. Supp. 2d 303, 307 (S.D.N.Y. 2010). Where a copyright owner has expended significant resources promoting products embodying its copyrights, losses resulting from infringement of such copyrights constitutes irreparable harm. *HarperCollins Publishers LLC, 721 F. Supp. 2d at 307; Ty, Inc. v. GMA Accessories, Inc*., 132 F.3d 1167, 1173 (7th Cir. 1997). A copyright owner's "invest[ment] of substantial time, effort and money into creating the [copyright-protected work]" coupled with the likely inability to realize the return on such investment due to infringement of the copyright, supports a finding of irreparable harm. *Ballas v. Tedesco,* 41 F.Supp. 2d 531, 542 (D.N.J. 1999). The sort of irreparable harm resulting from copyright infringement includes damage to the copyright owner's business reputation. *Spinmaster, Ltd. v. Overbreak LLC,* 404 F. Supp. 2d 1097, 1111 (N.D. Ill. 2005).

Since 2009, Plaintiff has invested substantial time, money, and effort creating and promoting Plaintiff's Products embodying the Copyright-Protected Images. (Li Decl. ¶ 22). Defendant's unauthorized use of the Copyright-Protected Images has and continues to irreparably harm Plaintiff through diminished goodwill and brand confidence, damage to Plaintiff's reputation, loss of exclusivity, and loss of future sales. (Li Decl. ¶ 23). The extent of the harm to Plaintiff's reputation, the goodwill associated therewith, and the possible diversion of customers due to loss

in brand confidence are irreparable and incalculable, thus warranting an immediate halt to Defendant's infringing activities through injunctive relief. (Li Decl. ¶ 24). See *Promatek Industries, Ltd. v. Equitrac Corp*., 300 F.3d 808, 813 (7th Cir. 2002) (finding that damage to plaintiff's goodwill was irreparable harm for which plaintiff had no adequate remedy at law). Plaintiff will suffer immediate and irreparable injury, loss, or damage if an *ex parte* Temporary Restraining Order is not issued in accordance with Federal Rule of Civil Procedure 65(b)(1). (Id. ¶ 15).

D. The Balancing of Harms Tips in Plaintiff's Favor, and the Public Interest Is Served by Entry of the Injunction.

As noted above, if the Court is satisfied that Plaintiff has demonstrated (1) a likelihood of success on the merits, (2) no adequate remedy at law, and (3) the threat of irreparable harm if preliminary relief is not granted, then it must next consider the harm that Defendant will suffer if preliminary relief is granted, balancing such harm against the irreparable harm Plaintiff will suffer if relief is denied. *Ty, Inc. v. Jones Grp., Inc*., 237 F.3d 891, 895 (7th Cir. 2001). The threat of continued copyright infringement without issuance of an injunction as well as the copyright owner's loss of exclusivity occasioned by copyright infringement support a finding that the balance of hardships weighs in favor of awarding injunctive relief. *Virtual Studios, Inc. v. Beaulieu Grp.,* LLC, 987 F. Supp. 2d 769, 781 (E.D. Tenn. 2013).

Defendant has been profiting and continues to profit from the sale of competing and Infringing Products. (Li Decl. ¶ 26). In so doing, Defendant has eliminated the exclusivity that Plaintiff was entitled to under the Copyright Act. (Li Decl. ¶ 27). Thus, the balance of hardships tips decisively in Plaintiff's favor. As such, equity requires that Defendant be ordered to cease its unlawful conduct.

IV. THE EQUITABLE RELIEF SOUGHT IS APPROPRIATE

A. Temporary Restraining Order Immediately Enjoining Defendant's Unauthorized and Unlawful Use of Plaintiff's Copyright-Protected Images Is Appropriate.

Plaintiff requests a temporary injunction requiring the Defendant to immediately cease all use of the Copyright-Protected Images on or in connection with all Defendant Internet Stores. Such relief is necessary to stop the ongoing harm to Plaintiff and to the goodwill attached to Plaintiff's Products embodying the Copyright-Protected Images, and to prevent the Defendant from continuing to benefit from its unauthorized use of the Copyright-Protected Images. The need for *ex parte* relief is magnified in today's global economy where infringers can operate anonymously over the Internet. Plaintiff is currently unaware of the scope and volume of Defendant's operations, nor how many other Defendant Internet Stores are used to sell and distribute the competing and Infringing Products. Courts ordinarily authorize immediate injunctive relief in cases involving the unauthorized use of another intellectual property and counterfeiting. See, e.g., *Entm't One UK Ltd. v. 2012Shiliang*, 384 F. Supp. 3d 941, 947 (N.D. Ill. 2019); see also *Sugartown Worldwide LLC v. The Partnerships and Unincorporated Assocs. Identified on Schedule A, Cas*e, No. 20-cv-5183 (MSS), D.I. 70 (Sept. 18, 2020) (TRO Order).

B. Plaintiff will post a security bond in accordance with this Court's Orders.

The posting of security upon issuance of a temporary restraining order or preliminary injunction is vested in the Court's sound discretion. *Rathmann Grp. v. Tanenbaum*, 889 F.2d 787, 789 (8th Cir. 1989); *Hoechst Diafoil Co. v. Nan Ya Plastics Corp*., 174 F.3d 411, 421 (4th Cir. 1999); Fed. R. Civ. P. 65(c). Because of the strong and unequivocal evidence supporting its claims for copyright infringement, and unfair competition, Plaintiff respectfully requests that this Court require Plaintiff post a bond of no more than One Thousand Dollars and Zero Cents in United

States currency ($1,000.00 USD) as security in this action. Similar bonds have been authorized in actions commenced in this judicial district to guard against the improper issuance of injunctive relief where a high likelihood of success on the merits has been demonstrated. Accordingly, Plaintiff submits that the same amount of security is appropriate in this action.

C. Plaintiff is Entitled to Expedited Discovery.

The United States Supreme Court has held that "federal courts have the power to order at their discretion, the discovery of facts necessary to ascertain their competency to entertain the merits." *Vance v. Rumsfeld*, No. 1:06-cv-06964, 2007 WL 4557812, at *6 (N.D. Ill. Dec. 21, 2007) (quoting Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351, 98 S. Ct. 2380 (1978)). Courts have wide latitude in determining whether to grant a party's request for discovery. *Id*. (citation omitted). Further, courts have broad power over discovery and may permit discovery in order to aid in the identification of unknown defendants. See Fed. R. Civ. P. 26(b)(2). Plaintiff respectfully requests expedited discovery to discover bank and payment system accounts Defendant uses for its infringing sales operations, as well as the IP addresses Defendant uses to login and access their Stores and Accounts. The financial accounting records will allow Plaintiff to gauge the extent of Defendant's infringing activities. The expedited discovery requested in Plaintiff's Proposed TRO is limited to include only what is essential to prevent further irreparable harm. Accordingly, Plaintiff respectfully requests that expedited discovery be granted.

V. CONCLUSION

Defendant's infringement of Plaintiff's Copyright-Protected Images is impinging upon the exclusivity that Plaintiff is entitled to under the Copyright Act. Without entry of the requested relief, Defendant's sale of competing products and unauthorized use of Plaintiff's Copyright-Protected Images will continue to harm Plaintiff in ways not compensable monetarily. Defendant's

infringing operations are irreparably harming Plaintiff's business, its business reputation, and its marketplace goodwill. Entry of an *ex parte* order is necessary. Plaintiff respectfully requests that this Court enter a Temporary Restraining Order Enjoining Defendant's reproduction, public display, and distribution of Plaintiff's Copyright-Protected Images and all other activity by Defendant that would constitute an infringement of Plaintiff's copyrights asserted in this action.

DATED: July 3, 2025

Respectfully submitted,

By: */s/ Katherine M. Kuhn*

Katherine M. Kuhn (Bar No. 6331405)
Joseph W. Droter (Bar No. 6329630)
BAYRAMOGLU LAW OFFICES LLC
233 S. Wacker Drive, 44th Floor, #57
Chicago, IL 60606
Tel: (702) 462-5973 Fax: (702) 553-3404
Katherine@bayramoglu-legal.com
Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on the 3rd day of July 2025, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Northern District of Illinois, Eastern Division, using the electronic case filing system. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means. Notice of this filing is provided to unrepresented parties for whom contact information is listed below and provided via email and by posting the filing on a URL contained on our website http://blointernetenforcement.com, and a link to said website in the email provided by third-party platform.

Respectfully submitted,

By: */s/ Katherine M. Kuhn*
Katherine M. Kuhn (Bar No. 6331405)
BAYRAMOGLU LAW OFFICES LLC
233 S. Wacker Drive, 44th Floor, #57
Chicago, IL 60606
Tel: (702) 462-5973 Fax: (702) 553-3404
Katherine@bayramoglu-legal.com
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HONG KONG LEYUZHEN TECHNOLOGY CO. LIMITED, Plaintiff, v. Shenzhen Yilanya Technology Co., Ltd., Defendants.	**Case No.: 1:25-cv-04947-MMP-HKM** **Honorable Martha M. Pacold** **Magistrate Heather K. McShain**

DECLARATION OF KATHERINE M. KUHN, ESQ. IN SUPPORT OF PLAINTIFF'S *EX PARTE* MOTION FOR ENTRY OF A TEMPORARY RESTRAINING ORDER

I, Katherine M. Kuhn, of the City of Chicago, in the State of Illinois, declare as follows:

1. Except as otherwise expressly stated to the contrary, this declaration is based upon my personal knowledge of the following facts and, if called as a witness, I could and would competently testify to the statements made herein.

2. I make this declaration in support of Plaintiff's Motion for Entry of a Temporary Restraining Order, including a temporary injunction, and expedited discovery.

3. I am an attorney at law, duly admitted to practice before the Courts of the State of Illinois and the United States District Court for the Northern District of Illinois. I am one of the attorneys for Plaintiff Hong Kong Leyuzhen Technology Co. Limited ("Plaintiff"). In my experience in combating online infringement as an intellectual property attorney, I am knowledgeable about key aspects of intellectual property protection including, but not limited to, trademarks, copyrights, other intellectual property, sales, on-line sales, and associated

international operations. I make this declaration from my matters within my own knowledge unless stated otherwise.

4. According to a January 2011 MarkMonitor report entitled "Traffic Report: Online Piracy and Counterfeiting," the combined traffic to 48 sites selling counterfeit goods was more than 240,000 visits per day on average or more than 87 million visits per year. A 2012 MarkMonitor article entitled "White Paper: Seven Best Practices for Fighting Counterfeit Sales Online" reported that counterfeiters' illicit online activities will cost legitimate businesses billions in lost revenue annually. True and correct copies of these reports are attached hereto as **Exhibit 1**.

5. According to an intellectual property rights seizures statistics report issued by the U.S. Customs and Border Protection agency of the U.S. Department of Homeland Security, the manufacturer's suggested retail price of goods seized by the U.S. government in fiscal year 2020 was over $1.3 billion. A true and correct copy of this report is attached hereto as **Exhibit 2**. A 2016 report by Business Action to Stop Counterfeiting and Piracy ("BASCAP") and the International Trademark Association ("INTA") entitled "The Economic Impacts of Counterfeiting and Piracy" included findings that counterfeit and pirated products account for an estimated $461 billion in losses in international trade in 2013, resulting in tens of thousands of lost jobs for legitimate businesses and broader economic losses, including lost tax revenue. These figures are expected to increase each year. A true and correct copy of this report is attached hereto as **Exhibit 3**.

6. A true and correct copy of the Internet Corporation for the Assigned Names and Numbers ("ICANN") Registrar Accreditation Agreement is attached hereto as **Exhibit 4**. According to section 3.3 of the Registrar Accreditation Agreement established by ICANN, an

individual or entity that registers a domain name is required to provide, on an interactive web page, its accurate contact details including a valid email and mailing address, amongst other information.

7. Undersigned counsel performed, supervised, and/or directed investigations related to Internet-based infringement of the Rotita Copyrights. To date, our investigation shows that Infringers are using Online Stores to sell competing Rotita products from foreign countries such as China to consumers in the U.S. and elsewhere while using, without authorization, the Rotita Brand Copyrights to do so. I have directly (or someone working under my direction supervision has) analyzed the Defendant's Online Stores and determined that the stores were using the Rotita Copyrights without authorization to offer competing Rotita Brand products of inferior quality for sale to consumers in the United States, including to consumers in the State of Illinois. This conclusion was reached through visual inspection of the products listed for sale on Defendant's Online Stores, the price at which the competing Rotita Brand products were offered for sale, and other features commonly associated with websites selling competing, counterfeit and/or knockoff products.

8. True and correct copies of screenshot printouts showing Defendant's Online Stores on which the Rotita Copyrights are displayed without authorization, as well as pages confirming the ability to order and ship competing Rotita Brand products to the United States are attached as **Exhibit 5**.

9. Upon information and belief, Infringers typically set up online stores on well-known e-commerce platforms and, to unknowing consumers, appear to be authorized online retailers, outlet stores, or wholesalers selling genuine counterfeit products. Defendant's Online Stores appear sophisticated and accept payment in U.S. dollars via credit cards, and PayPal. Defendant's Online Stores often include images and design elements that make it very difficult for

consumers to identify them as counterfeit or unauthorized knockoff brand sellers. Defendant therefore perpetuates the illusion of legitimacy by using indicia of authenticity and security that consumers have come to associate with authorized online retailers. Plaintiff has not licensed or authorized Defendant to use the Rotita Copyrights, and the Defendant is not authorized to use the copyright protected works at issue in this action.

10. Defendant deceives unknowing consumers by using photographs and 3-D artwork contained in the Rotita Copyrights without authorization within the content to attract various search engines crawling the Internet looking for websites relevant to consumer searches for Rotita Brand products. Additionally, Defendants typically use other unauthorized search engine optimization ("SEO") tactics and social media spamming so that the Defendant's listings show up at or near the top of relevant search results and misdirect consumers searching for genuine Rotita Brand products. Further, Defendants typically utilize similar illegitimate SEO tactics to propel new domain names to the top of search results after others are shut down.

11. Upon information and belief, Defendant has gone, and defendants in similar cases go to great lengths to conceal their identities and often use multiple fictitious names and addresses to register and operate their massive network of online stores. For example, many of Defendants' names and physical addresses used to register Defendants' Online Stores are incomplete, contain randomly typed letters, or fail to include cities or states. Defendants in similar counterfeit and knockoff product cases, also use privacy services that conceal the owners' identity and contact information and regularly create new websites and online marketplace accounts on various platforms, using the name Shenzhen Yilanya Technology Co., Ltd., as well as other unknown fictitious names and addresses. Such Internet store registration patterns are one of many common

tactics used by defendants to conceal their identities, the full scope and interworking of their massive counterfeiting operation, and to avoid being shut down.

12. In addition to operating under multiple fictitious names, Defendant in this case and defendants in other similar cases against online counterfeiters or knockoff sellers use a variety of other common tactics to evade enforcement efforts. For example, sellers like Defendant will often register new domain names or online marketplace accounts under new aliases once they receive notice of a lawsuit. Infringing sellers also often move website hosting to rogue servers located outside the United States once notice of a lawsuit is received. Infringers also typically ship products in small quantities via international mail to minimize detection by U.S. Customs and Border Protection.

13. Based on my experience in investigating counterfeit and knockoff products, including the instant investigation, sellers such as Defendant typically operate multiple credit card merchant accounts, such as Alipay and PayPal, hidden behind layers of payment gateways so that they can continue operation despite legal enforcement efforts. Further, defendants, such as the Defendant in this case, typically maintain offshore bank accounts and regularly move funds from their various e-commerce accounts to these offshore accounts because they are outside the jurisdiction of United States' courts, such as this Court.

14. Defendant in this case, willfully and without authorization, use the Rotita Copyrights to promote, advertise, offer to sell, and sell competing, poor quality goods through its Alibaba stores. Defendant is creating a false association in the minds of consumers between the illegitimate websites and the authorized, legitimate Rotita Brand retailer by deceiving consumers through, among other things, the unauthorized display of the Rotita Copyrights. These circumstances justify entry of a temporary restraining order to immediately stop

the Defendant from improperly benefiting from its unauthorized use of the Rotita Copyrights and to preserve the status quo until a hearing can be held in this matter. As of the date of this filing, the link identified in Plaintiff's First Amended Complaint is still active and displaying Plaintiff's Copyright Protected Images [Dkt. No. 22-5],

15. In addition to having developed a sophisticated online sales network, the Defendant is most likely a part of a network exceptionally skilled at identifying plaintiffs, their allegedly infringed products, immediately disseminating this information throughout their network by posting on online websites such as "SellerDefense.cn."

16. Absent entry of a temporary restraining order without notice, Defendant can, and likely will, modify registration data and content, change hosts, redirect traffic to other websites under its control, and/or move any assets from U.S.-based bank accounts to offshore accounts.

17. Defendant's Online Stores have been registered with the identified Alibaba platform, which helps to increase its anonymity by interposing a third party between the consumer and Defendant. Expedited discovery is required to discover confirmed contact information, origin of infringement, bank and payment-system accounts used by Defendant in furtherance of understanding the extent of the effect on Rotita sales operations. In this regard, Plaintiff's expedited discovery requested in its Proposed Temporary Restraining Order has been limited to include that which is only necessary to prevent further irreparable harm.

18. As Defendant has engaged in many deceptive practices in hiding its identities, accounts and inter-workings of its operations, Plaintiff's Proposed Temporary Restraining Order may have little meaningful effect without also being able to serve necessary discovery, through Federal Rule of Civil Procedure 45 or otherwise, on third parties potentially associated or acting in concert with the Defendant. As such, Plaintiff requests that it additionally be permitted to engage

in third party discovery to the extent necessary to effectuate the narrow scope of inquiry identified above.

19. Further, it is respectfully submitted that *ex parte* relief is necessary to avoid immediate and irreparable injury. Indeed, if Defendant were to learn of these proceedings prematurely, the likely result would be the destruction of relevant documentary evidence, which would frustrate the purpose of the underlying law and would interfere with this Court's ability to grant relief. Specifically, it appears that the Defendant in this case holds most of its data and assets in the Republic of China or Hong Kong, making it easy to hide or dispose of assets.

20. Plaintiff will suffer immediate and irreparable injury, loss, or damage if an *ex parte* Temporary Restraining Order is not issued.

I declare under penalty of perjury under the laws of the United States of America the foregoing is true and correct.

Executed on July 3, 2025 in Chicago, Illinois.

Respectfully Submitted

By: */s/ Katherine M. Kuhn*
Katherine M. Kuhn, Esq.

CERTIFICATE OF SERVICE

I hereby certify that on the 3rd day of July 2025, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Northern District of Illinois, Eastern Division, using the electronic case filing system. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

By: */s/ Katherine M. Kuhn*
Katherine M. Kuhn (Bar No. 6331405)
BAYRAMOGLU LAW OFFICES LLC
233 S. Wacker Drive, 44th Floor, #57
Chicago, IL 60606
Tel: (702) 462-5973 Fax: (702) 553-3404
Katherine@bayramoglu-legal.com
Attorneys for Plaintiff

EXHIBIT 1

January 2011

Traffic Report: Online Piracy and Counterfeiting

MarkMonitor®

Traffic Report: Online Piracy and Counterfeiting

Contents

The Internet is arguably one of the greatest innovations of modern society—allowing for countless new businesses to thrive and dramatically altering the way society operates. The Internet has enabled a global marketplace to flourish with lightning-quick communication and an unparalleled access to information. However, the advancement of the Internet into nearly all of our daily activities, combined with rapid download speeds, the perfection of digital copies, the rise of e-commerce and the complexity of online enforcement, has magnified the seriousness and consequences of online counterfeiting and piracy. Websites offering pirated goods generate billions of visits annually, and websites that sell counterfeit luxury goods, fake drugs, and products that may pose health and safety risks attract hundreds of millions annually.

"As our economy has worsened, brand abusers have sharpened their focus."

Recognizing that illicit online sales have a significant impact on the U.S. economy in financial terms as well as in public health and well-being, MarkMonitor® worked to identify a sample of rogue Internet sites that are responsible for trafficking counterfeit and pirated goods. The goal of the project was to illustrate the nature of this illicit ecosystem and, using publicly-available traffic information on the number of visits, determine its scope.

The first step was to identify business categories and brands targeted by online counterfeiters and digital pirates. Using 22 major brands as criteria—ranging from pharmaceuticals, luxury goods, and apparel to entertainment titles and software—MarkMonitor used its patented technology to comb the Internet for sites suspected of offering counterfeit goods or pirated digital content. The initial scans resulted in more than 10,000 results which were then de-duplicated and filtered further using MarkMonitor technology to identify dedicated e-commerce and digital download sites. The final step required hand-examination and verification of more than 600 results to determine classification. Since some sites offered multiple brands, this step led to almost 100 unique domains or websites which were then classified in one of two ways: 'counterfeit' or 'digital piracy'.

Using publicly-available Internet traffic data from Alexa, the sites were then ranked by the number of visits, which were significant, speaking to the level of demand for these goods as well as to the website operators' success in promoting these sites so they are visible and accessible online. Since the study used a sample of only 22 brands, it provides a small glimpse of the nature of online intellectual property (IP) theft and the dark side of illicit e-commerce. However, given the large number of popular brands, it is reasonable to assume that hundreds of thousands of other rights-holders, brands and content creators are suffering the same damage.

Key Findings

The study's findings demonstrate that online distribution of pirated digital content and e-commerce sales of counterfeit goods is rampant. Specific findings include:

- In total, the 10 media brands in the study yielded 43 unique sites classified as 'digital piracy.' Traffic generated to these sites was over 146 million visits per day, representing more than 53 billion visits per year.
- The top-three websites classified as 'digital piracy'—rapidshare.com, megavideo.com, and megaupload.com—collectively generate more than 21 billion visits per year.
- The availability of reliable infrastructure is an important factor in the location of sites hosting piracy. The study found that North America and Western Europe represented the host location for 67 percent of the sites classified as 'digital piracy.'
- The combined traffic to the 48 sites selling counterfeit goods is more than 240,000 visits per day on average or more than 87 million visits per year.
- When it comes to host location of the sites categorized as 'counterfeit', 73 percent were hosted in North America or Western Europe. Eastern European countries hosted another 14 percent of the sites while 9 percent of the sites were hosted in Asia.
- The combined traffic to the 26 sites selling counterfeit prescription drugs is more than 141,000 visits per day on average or more than 51 million visits per year.
- The combined traffic to the 21 e-commerce sites selling counterfeit luxury goods is more than 98,000 visits per day on average or almost 36 million visits per year.

"The study used only 22 brands, so we can assume that many other brands and content-creators are suffering similar damage."

These findings are just the tip of the iceberg. The true scope of the problem is exponentially higher in terms of user traffic, lost revenue and risks to public health and safety.

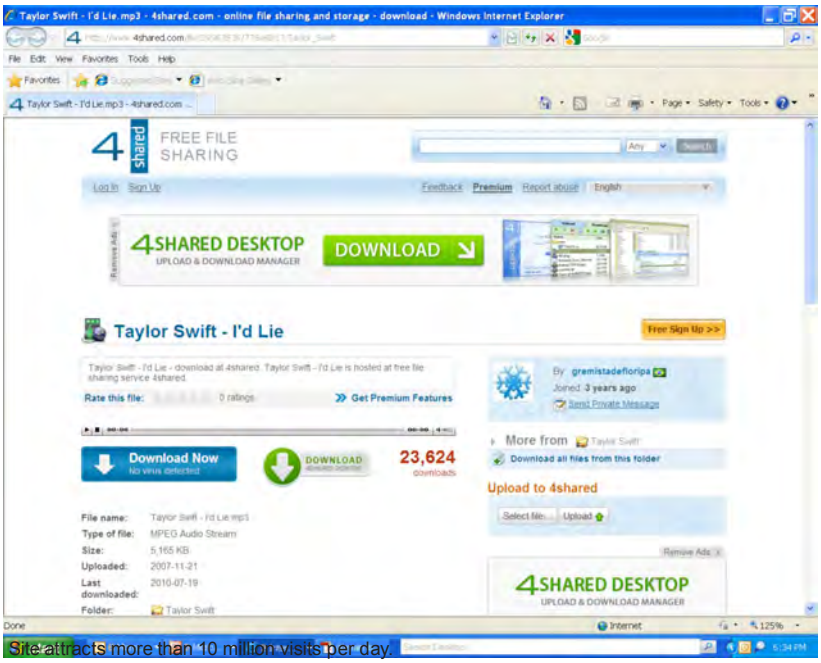
Methodology

Using a list of industries most affected by online counterfeiting and digital piracy,[1] MarkMonitor chose major brands from each industry and ran automated scans for those brands using its patented technology. In all, the study examined 22 brands in the digital content category (movies/TV shows, music and software/videogames) and the physical goods category (handbags, sports apparel, pharmaceuticals and luxury items, footwear, and apparel.)

The study used very narrow criteria to classify sites selling physical goods as 'counterfeit.' It is important to point out that many of the e-commerce sites that did not meet that strict guideline did display multiple factors arousing suspicion. This

[1] ~~Digital Content~~ industries: Entertainment (music/movies/television shows), Software/Videogames; Physical Goods: Handbags, Sports Apparel with logos, Pharmaceuticals, luxury items, footwear, and apparel.

underscores the crucial role that brand owners and law enforcement personnel trained by brand owners play in determining whether a site is offering counterfeit goods. Technology can be used to conduct the heavy lifting in identifying and prioritizing sites for further action, but the in-depth market and product knowledge of brand owners' is vital.



Site attracts more than 10 million visits per day.

The scans focused on identifying e-commerce and peer-to-peer, streaming, and torrent sites that yielded high traffic levels. In order to be classified as an e-commerce site, the site needed to contain a shopping cart while the sites classified as piracy needed to contain some type of link, index or player that could be used to download, stream or share digital content. These criteria were designed to eliminate editorial, blog or discussion sites and to focus exclusively on sites where pirated goods could be shared, viewed, streamed or downloaded and counterfeit goods could be purchased.

The initial scans resulted in more than 10,000 results which were then de-duplicated and filtered further using MarkMonitor technology to identify dedicated e-commerce and digital content sites used for downloading, sharing or streaming. The final step required hand-examination and verification of more than 600 results to determine classification. Since some sites offered multiple brands, this step led to almost 100 unique domains or websites which were then classified as either 'counterfeit' or 'digital piracy'. The results were ranked by the amount of traffic, defined as the number of daily visits, using Alexa-supplied information. None of the scans contained MarkMonitor customer data or information.

Criteria for Websites

The results from the initial scans were examined further by MarkMonitor experts in order to classify these sites, or domains, into one of two categories: 'counterfeit' or 'digital piracy.' After thorough analysis, MarkMonitor concluded that 91 websites with high traffic numbers qualified for inclusion in one of these categories. The 'counterfeit' classification referred to e-commerce sites selling counterfeit physical goods while the 'digital piracy' classification refers to sites offering pirated versions of music, movies, television shows, software, and videogames.

Digital Piracy: The total number of unique domains identified as 'digital piracy' totaled 43. To fit the 'digital piracy' classification, the domain needed to offer or point to one or more of the brands used in the digital content portion of the study for free. While some of these sites do offer takedown processes for pirated

content, the action must be initiated by the content owner. The resulting domains were then sorted by traffic volume.

'Counterfeit': In the case of e-commerce domains selling physical goods, the domains needed to satisfy one of two conditions to be deemed as selling counterfeit goods: (1) either the domain itself specified that the goods were not authentic (i.e., using terms like 'replica," 'knock-off,' and 'copy') or (2) in the case of pharmaceuticals, the domain offered 'generic' versions of prescription drugs that are not available in generic form in the U.S., targeted the U.S. market by providing pricing in U.S. currency, and did not require a prescription.[2] Since some domains offered more than one type of product, the domain is counted only once, even if multiple URLs for that domain surfaced during the scans. MarkMonitor found that 48 websites fell under the criteria for selling counterfeit goods.

While the online pharmacies displayed the 'generic' label prominently on product listings, MarkMonitor needed to consult FAQ or 'About' sections of the online drugstores, or even needed to follow the purchase process, in order to determine if prescriptions were required by the online pharmacy. In addition, MarkMonitor examined the currency used to quote prices, shipping information or other information on the site that indicated markets served, such as flags, shipping information, telephone numbers or references to the U.S. Drug Enforcement Agency. Many of the e-commerce domains selling counterfeit goods displayed the term 'replica' quite prominently while others included such information in their FAQ or 'About.'

Site sells 'generics' without prescription for prescription drugs that are not available in generic form.

Site explains the difference between 'generic' and branded prescription drugs and highlights unmarked shipping envelopes.

[2] During the course of the study, MarkMonitor identified some additional sites that fit the criteria for inclusion but did not use one of the original media brands such as sites offering key generators used to 'unlock' protected material.

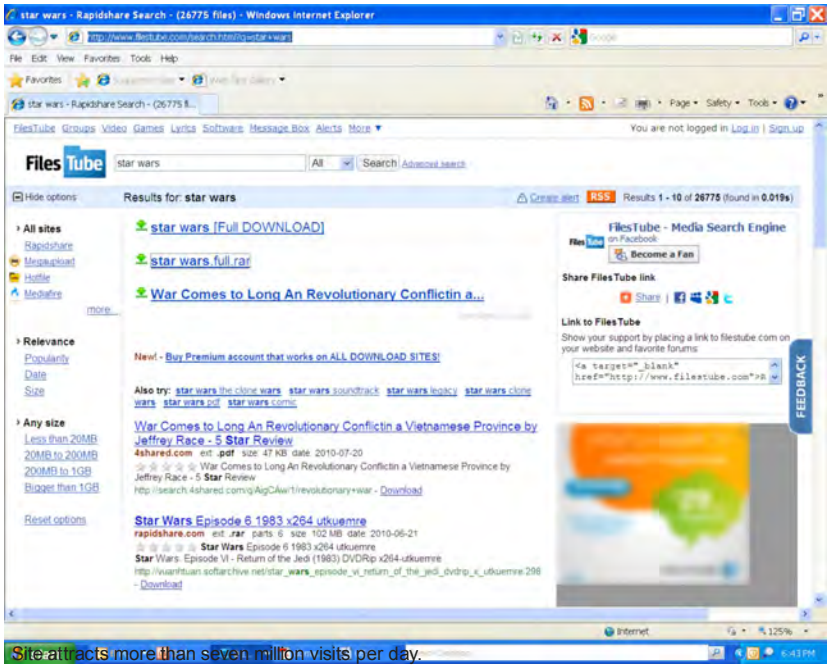
Traffic Analysis

As a backdrop to examining website traffic figures, it is important to point out that traffic measurements can vary greatly depending on methodology. Some traffic measurement sources depend on technology, others depend on some type of user panel or community, and a third category uses a hybrid approach. Each approach has advantages and disadvantages which, as a result, allow publicly-available traffic data to vary based upon the measurement source. In this study, MarkMonitor used data based on Alexa. The more than 90 unique domains culled from the initial set of over 10,000 results display a wide range of traffic figures, depending on the type of goods being offered.

> *"Traffic to sites suspected of offering pirated content was over 146 million visits per day."*

Digital Piracy Web Traffic Analysis: Those domains classified as 'digital piracy' attracted the highest levels of traffic with a high in excess of 32 million daily visits on average for the most-trafficked domain—rapidshare.com. On an annual basis, that traffic equates to more than 11.8 billion visits per year for that site. This pattern continues with the second and third most-trafficked sites—megavideo.com and megaupload.com—each of which generates more than 13 million visits per day on average, or more than 4.9 billion visits per year to each site. Collectively, these three digital piracy sites generate more than 21 billion visits per year.

In total, traffic generated to the sites classified as 'digital piracy' was more than 146 million visits per day, representing more than 53 billion visits per year. Lest these figures be viewed as anomalies, examining the ten least-visited 'digital piracy' sites show annual visits total more than 781 million per year, demonstrating that even the lesser-trafficked sites in this category drive significant traffic.



Site attracts more than seven million visits per day.

The bulk of the 'digital piracy' sites, or 67 percent, were hosted in North America or Western Europe.

Counterfeit Website Traffic Analysis: Due to the narrow criteria used to classify sites as 'counterfeit,' all the sites included in the analysis, with one exception, sold prescription drugs or luxury goods, including handbags, watches or jewelry. The combined traffic to the 48 sites selling counterfeit goods is more than 240,000 visits per day on average or more than 87 million visits per year. The majority of these sites reflect similar patterns as the sites classified as 'digital piracy' when it comes to the server's host location with or 56 percent hosted in North America and Western Europe. However, Eastern European countries hosted 22 percent of the sites while 14 percent of the sites were hosted in Asia.

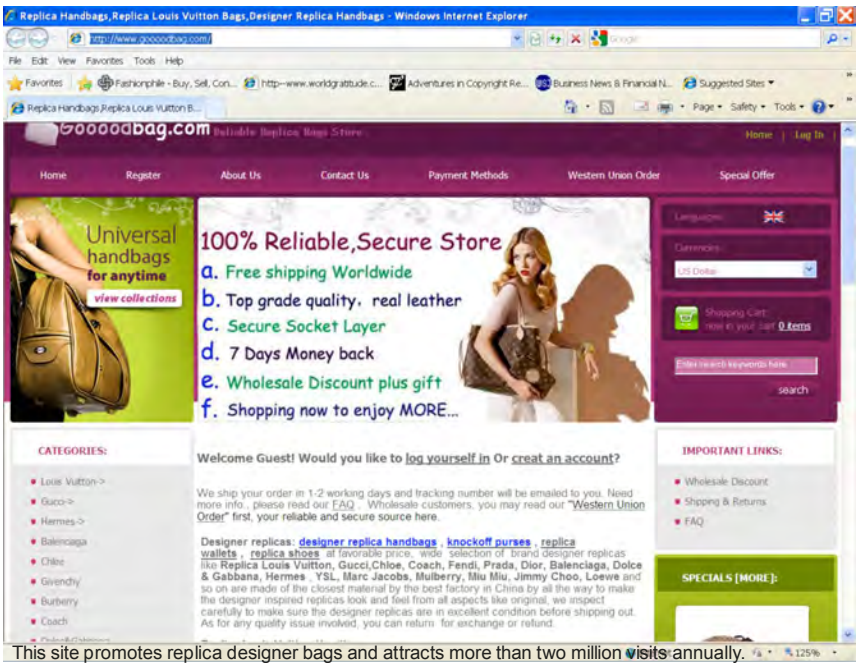
However, examining the site registration information for these 'counterfeit' sites suggests that more of these sites may be linked to Asia as seven sites hosted in non-Asian countries are actually registered by Asian registrars. Factoring in that information indicates that 29 percent of the sites have some connection to Asia, either through host location or registrar.

While not at the scale of the suspected digital piracy sites, e-commerce domains classified as 'counterfeit' attracted considerable levels of traffic as well with the most-trafficked site, an Internet pharmacy, driving 28,000 daily visits on average, representing more than 10 million visits to the site per year.

> *"Combined traffic to the sites selling counterfeit goods is more than 87 million visits per year."*

Suspicious Sites: During the course of the research, we identified sites that displayed one or more factors that appeared questionable, such as significant price discounts, links to sites selling counterfeit goods, trade dress issues, or, in the case of online pharmacies, no requirement for prescriptions. These types of issues underscore the crucial role that brand owners and law enforcement personnel trained by brand owners play in determining whether a site is offering counterfeit or pirated goods. While some sites are very clear in specifying their goods are 'copies' or 'replicas,' others are less forthcoming. In many cases, deep discounts combined with promises of high-quality goods from the current season raise questions that only the brand owner—with knowledge of channel strategy, pricing and partnerships—can address.

In the case of highly regulated goods like pharmaceuticals, intellectual property protections for pharmaceutical patents or regulations governing generics may differ across national boundaries. Instead, the business practices of the pharmacy itself—such as prescription requirements or sales of individual pills—are more useful in identifying suspicious drugs. The role of the brand owner, with in-depth knowledge of distribution channels, pricing and local business practices, is vital. In each of these examples, the most authoritative answer is provided by a physical examination of the goods themselves.



This site promotes replica designer bags and attracts more than two million visits annually.

Conclusion

The research presented in this study demonstrates the wide availability of pirated digital content and counterfeit goods via the Internet and e-commerce. The websites yielded in the research and analyses of this study all have one thing in common: business models that are indisputably centered on the sale or distribution of counterfeit and pirated goods. These illegal operations are shifting revenue

from legitimate brands' e-commerce sites, causing economic harm and risking consumer health. This study highlights the type of data that needs to be examined in order to identify and locate sites trafficking in counterfeit and pirated goods. Accurate and unbiased information describing the scope of online counterfeiting and piracy as an essential prerequisite for safeguarding consumer safety and economic well-being.

While counterfeiting and piracy in the physical world are serious problems, these issues are growing at a significant rate online and pose unique challenges in remediation, due to the inherent nature of the Internet with its global reach, cost efficiencies, and anonymity. Awareness and educational efforts focused on the distinctive nature of online counterfeiting and piracy are necessary in developing effective response mechanisms to this global, cross-border problem. Necessary government policies, corrective legislative measures, law enforcement action and, most importantly, actively-engaged brand owners are all needed to stem this growing tide of illegal Internet activity. The bottom line is that online IP theft ultimately affects the most creative and innovative sectors of the economy, contributing to billions in lost revenue and millions of lost jobs. Protecting IP rights is a critical component of our economic resurgence, and vitally important to our future; stopping the spread of pirated and counterfeit goods is a necessity.

> *"Combined traffic to the pharmacies selling suspected counterfeit prescription drugs is more than 51 million visits per year."*

About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its patented real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today. For more information, visit **www.markmonitor.com**

More than half the Fortune 100 trust MarkMonitor to protect their brands online.
See what we can do for you.

MarkMonitor, Inc.
U.S. (800) 745.9229
Europe +44 (0) 207.840.1300
www.markmonitor.com

MarkMonitor®

White Paper

Seven Best Practices for Fighting Counterfeit Sales Online

Executive Summary

Counterfeit sales represent seven percent of all global trade.[1] The damage these sales do to rightful brand owners goes well beyond revenues and profits: Numerous reports have suggested that counterfeit and piracy trade supports terrorism, organized crime and other threats to both national security and human rights. The Internet's rapid growth — along with its instant global reach and anonymity — has significantly escalated the situation.

An entire online supply chain, parallel to legitimate distribution channels, has flourished around counterfeit goods. Online B2B marketplaces, in addition to e-commerce sites — many promoted via social media and search engines — commonly traffic in counterfeit goods. Fake products acquired on wholesale sites are sold across multiple digital channels, or at flea markets and shops in the physical world.

Deceptive use of proven marketing techniques — paid search ads, search engine optimization, email and social media campaigns, branded domain names and more — are important parts of this illicit ecosystem, as savvy counterfeiters apply marketing best practices.

Fortunately, brand owners can adopt their own proven best practices to successfully combat online counterfeit sales. Unlike anti-counterfeiting strategies in the physical world, however, a two-pronged approach is necessary: Brand owners must choke off counterfeit sales at both promotional and distribution points. Technology exists for identifying and quantifying worldwide online counterfeiting activity in both promotional and distribution channels, and, once visible, infringement can be prioritized and attacked. The battle against online counterfeit sales can be won. With billions in revenues, critical customer loyalty and even public safety and human rights at stake, it must.

Contents

Counterfeiting: A Growing Online Threat

"If you can make it, you can fake it." Unfortunately, the old saying is all too true. Sales of counterfeit goods affect a wide range of industries, from high-margin luxury and technology goods to low-margin consumer goods like batteries, shampoo, gasoline and food.

The problem is growing, in part because the volume of fake goods produced is rapidly increasing — especially in countries like China, where manufacturing capacities continue to skyrocket. Mainland China was the point of origination for approximately $1.2 billion of the $1.7 billion in counterfeit goods confiscated by U.S. law enforcement agencies in 2013.[2]

This growth in supply helps fuel the exploding demand — especially online. The Internet's rapid growth — along with its instant global reach and anonymity — has significantly escalated the situation, moving the sale of counterfeit goods from the local street corner to a global marketplace. Because criminals can quickly and easily set up e-commerce storefronts or place listings on B2B marketplaces cost-effectively, their activities will continue to cost legitimate businesses billions in lost revenue.

Counterfeiting's Real Cost to Business

According to the secretary general of the ICC, multinational manufacturers lose roughly ten percent of their top-line revenue to counterfeiters — but the impacts go well beyond the revenue hit. For some companies, perceived brand value suffers when knock-offs become plentiful. Brands may even lose representation in distribution channels when resellers and affiliates see a reduction in demand due to competition from fakes. Additionally, the availability of cheaper, albeit fake, alternatives can exert downward pressure on legitimate brand pricing.

Other impacts include product safety issues — especially in pharmaceutical, automotive, aviation, healthcare, electronics and similar industries — accompanied by increased legal liability risks. And as consumers experience quality problems with fake goods, the legitimate brand's customer service and warranty costs can climb.

Marketing costs also rise as illicit sellers bid up paid search advertising costs and erode legitimate search engine optimization (SEO) investments. Finally, as more customers encounter inauthentic brand experiences, both loyalty and lifetime customer value suffer.

How Counterfeiting Thrives Online

Counterfeits in Digital Channels Affect Multiple Industries:

Tablets	Listings for clones, suspected counterfeits or gray market tablet computers numbered more than 23,000 in a single day
	More than 6,600 cybersquatted sites taking advantage of tablet brands generated more than 75 million annual visits
Luxury Goods	Suspected counterfeiters attracted 120 million annual visits to their e-commerce sites, representing almost half the traffic generated by the legitimate dot com sites for five luxury brands
	Brandjackers set up more than 1,100 cybersquatted sites touting luxury brands and more than 50 suspicious vendors purchased luxury brands keywords in paid search scams
Sports Apparel	Suspected counterfeiters attracted 56 million annual visits to e-commerce sites annually
	Suspected counterfeiters sold almost 1.2 million suspicious jerseys via e-commerce and business-to-business (B2B) marketplaces sites annually
	We found more than 6,000 suspects selling more than 1.2 million shirts or jerseys annually over the Internet, generating nearly $25 million in revenue.

Source: MarkMonitor Brandjacking Index®

An entire online supply chain — parallel to legitimate distribution channels — has grown around counterfeit goods. This illicit but highly profitable industry takes advantage of the same online tools, techniques and best practices employed by legitimate brands online.

The contrasts with counterfeiting in the physical world are important to understand, and are based upon the Internet's global reach, anonymity and efficiency. These attributes — and especially the digital world's powerful promotional potential — have enabled online counterfeiters to dramatically (and rapidly) outstrip all the street corner fakes, flea markets and "Canal Street districts" that exist.

In the wholesale trade, B2B marketplaces (also known as trade boards) often traffic in counterfeit goods. At the retail level, counterfeiters also use marketplaces to supply counterfeit goods to consumers. It's not unusual for counterfeiters to acquire fake goods on wholesale sites, only to resell them to consumers via digital channels — in addition to offline flea markets, bazaars and even retail shops.

Promotion is an important part of this illicit ecosystem. Counterfeiters use the same tactics as legitimate marketers, such as paid search ads and search engine optimization to lure buyers to their sites. According to Direct Magazine, fully 14 percent of searches on a branded item lead online users somewhere other than the legitimate brand's site. While some of these searches may lead to legitimate resellers or partners, it's reasonable to assume that many of them end up on the site of a counterfeiter.

Some counterfeit sellers also employ unsolicited email — spam — to boost their site traffic. This is especially prevalent among sellers of fake pharmaceuticals, software and luxury goods such as watches, jewelry and high-end apparel. They also make use of cybersquatting techniques, using branded terms in domain names in order to attract Web traffic and convey authenticity. And, as savvy marketers, they take advantage of inbound linking strategies and other SEO techniques to sell their illicit goods online.

The counterfeiting ecosystem extends to popular auction and exchange sites where direct searches frequently include counterfeit goods among their results. Links to sites pushing counterfeit wares can also be found on social media venues such as social networking sites, blogs and micro-blogs.

Clearly, legitimate and counterfeit ecosystems overlap — with some auction and e-commerce sites selling both real and fake goods — and this makes the problem more difficult to address. There are best practices, however, which can help brands minimize the damage from counterfeit sales in digital channels.

Beating Back Counterfeiters Online: Seven Best Practices

While the sale of counterfeit goods in the physical world is a timeworn tradition — if an unwelcome one — the online counterfeiting ecosystem offers unique challenges that require a unique approach. Proven best practices have emerged from brands that have actively and successfully engaged in combating counterfeit sales online.

1. Attain global visibility. Before a brand can understand the scope of the threat posed by online counterfeit sales, it must expose and quantify the problem. Counterfeiters operate over a wide array of online channels; all of these, including online marketplaces, e-commerce sites, message boards and the rest, must be monitored and analyzed. There's some good news for brands, however. Our experience shows that ten online marketplaces account for fully 80 percent of all marketplace traffic. Monitor these marketplaces, and you're watching a significant share of traffic.

Counterfeiters depend on technology to drive sales volumes so approach the monitoring challenge with the same tools and leverage technology to form a complete and accurate picture of the counterfeiting challenge that your brand faces.

2. Monitor points of promotion. While it's obviously important to identify and shut down distribution channels, it's almost certain that counterfeiters will regularly seek new sales venues. So it's just as critical to monitor the online promotional channels used by these criminals.

Counterfeiters use the same effective promotion techniques employed by legitimate marketers while leveraging the powerful, highly recognizable brands built by experts. Using paid search advertising, links within social media, black hat SEO tactics, cybersquatting and spam, they successfully steer traffic to their illicit offerings, and diminish the marketing ROI of legitimate brands. Monitoring for these promotional efforts is critical — and enables our next best practice.

3. Take proactive action. Counterfeiters obviously encounter more success when left to operate unchallenged; they're also known to shift their energies to more passive targets when brands visibly fight back. Once a brand understands where

the greatest threats lie, aggressive action is the best strategy. Brands should:

- Set priorities. Identify the biggest offenders, offering the greatest number of counterfeit goods in the most highly trafficked venues, and address them first. Brand owners should determine which counterfeit goods are generating the largest sales, and target them first as well.
- Watch for cybersquatters. Brands should actively monitor the Internet for unauthorized use of their branded terms in domain names. This will aid in rapid detection of e-commerce sites selling counterfeit or unauthorized goods — and frequently also uncovers other abuses such as false association with offensive content like pornography.
- Become a difficult target. Brands that visibly, vigorously fight to remove counterfeit goods from online venues often see a dramatic drop in infringement against their brands.
- Use all your weapons. Most online channels provide mechanisms for dealing with counterfeit sales situations. Online marketplaces, for example, typically have policies and procedures enabling brand owners to report listings that infringe their brand.

Search engines offer similar facilities. Major search engines have procedures for requesting the removal of ads linked to counterfeit sites. Websites can also be removed from search results pages if they are found to violate copyright laws (a common practice among sites selling counterfeits, typically through unauthorized use of product images).

- Get help from friends. Industry relationships can be powerful weapons in the fight against online counterfeiting. When choosing a brand protection solution provider, look for one with established ties with thousands of ISPs and Registrars worldwide. Simply put, these ties make it possible to get counterfeit sites shut down more quickly—thereby minimizing brand owner losses. Trade associations such as the International AntiCounterfeiting Coalition (IACC), the Anti-Counterfeiting Group (ACG) and the American Apparel and Footwear Association (AAFA) also provide resources and advice on best practices for fighting counterfeiters.

The Best Tools for Fighting Technology-enabled Counterfeit Sales

Brand:	Snap-on
Challenge:	Significant online sales of counterfeit Snap-on tools, resulted in erosion of revenues, perceived brand value and customer loyalty.
Response:	Snap-on employed sophisticated monitoring and detection technology solutions to fight online counterfeit sales.
Results:	Counterfeit products valued at $1.2 million — found in 4,900 illegal auction listings — were identified and removed in coordination with an online auction site.

4. Fight online counterfeit sales holistically. Online counterfeit sales are easier to address when the entire enterprise participates. That means brand owners should set up a cross-functional task force to address the issue in a coordinated, holistic manner.

Stakeholders — and, therefore, recommended participants — will vary by industry and enterprise, but can include legal, marketing, risk management, loss prevention,

channel sales management, manufacturing, supply chain management and other functional units.

Because fighting online counterfeiting requires attacking both promotional and distribution channels, this group needs to address more facets of the problem than seen in the physical world. All of these groups can, and should, set priorities and strategies for detecting, reporting and responding to infringers and should continue to inform the process as their situations and perceptions dictate.

5. Let online intelligence inform offline defense measures. Because offline measures — physical investigations, factory raids and other activities — can be costly and time-consuming, it's critical to know where they should be focused. Online intelligence can help identify the most egregious infringers, so that offline defensive efforts can be focused where they'll be most effective.

6. Act swiftly — and globally. Perhaps even more than it affects legitimate business, the proliferation of international trade offers tremendous benefits to online counterfeiters. While a domestic seller or manufacturer may seem like an easy first target, brands have learned that it's more effective to launch global anti-counterfeiting initiatives — and to get them underway expeditiously.

Prepare by ensuring your trademarks are registered internationally — especially in China, which observes a "first-to-file" policy that grants registration to whoever files first, even if it's not the true brand owner.

A global effort doesn't preclude addressing markets that target a specific country exclusively. In some cases, this will require competent language translation resources for monitoring, detection and enforcement. Most companies rely on third-party brand protection solution providers for this kind of expertise.

7. Educate your customers. Your customers can be an important ally in minimizing sales of counterfeit goods with all its associated costs. Educate your customers about the risks of buying from unauthorized sources, and recruit them to join in the effort by reporting suspicious goods and sellers. The Authentics Foundation and its consumer site, dontbuyfakes.com, have useful resources for consumer education. Also, many brands provide form or email-based mechanisms for reporting suspected infringement. When offering such tools, be sure to reinforce the benefits of buying authentic goods from authorized sellers.

Footwear Manufacturer Stomps Online Counterfeiters

Global footwear leader Deckers Outdoor, faced with millions in online sales of counterfeit and grey market goods, moved promptly to protect its customers and its bottom line. Leveraging brand protection technology, the company was able to:

- Pinpoint — and remove or de-list — $4.35 million in illegitimate goods and knock-offs within just 90 days
- Significantly curtail counterfeiting activity that undermined its revenues
- Enhance its brand reputation and increase customer trust and loyalty by automating and extending online enforcement

Online Intelligence Helps Focus Physical Efforts

Acushnet Company, a leader in the golf industry, leveraged online intelligence to guide a major raid in the U.K., shutting down a large counterfeiting operation that fed online distribution channels.[3]

Conclusion: The Fight Is Yours to Win

Online counterfeiting can heavily impact any company, affecting revenues, channel relationships, customer experience, marketing effectiveness, legal liability and more. Ignoring it — or just hoping for the best — simply isn't good business.

Fortunately, taking action can be fairly straightforward. Implementing the best practices discussed here doesn't have to involve complex organizational changes or extensive hiring efforts, as third-party solution providers can help make the effort efficient and supplement internal teams.

To successfully reduce the negative effects of counterfeiting, many companies have found that a cross-functional team contributes a great deal to an aggressive, global anti-counterfeiting initiative.

Most importantly: To effectively choke off counterfeit sales, the strategy must focus on both distribution and promotional channels for counterfeit goods. The returns — in revenues, profits, and long-term brand value — will certainly make the effort worthwhile.

Global Imaging Giant Protects its Image — and Profits

Print technology leader Epson created a centralized mechanism for globally monitoring for online brand abuses including counterfeit sales.

By forming a global, cross-functional team, Epson achieved a three-fold reduction in counterfeit sales activities on consumer and B2B marketplaces. Their visible, aggressive strategy has also served to deter abuse.

Tall Order: Fighting Counterfeiting in China

One of the most important centers of counterfeit trade is China. In addition to originating roughly $1.2 billion of the $1.7 billion in counterfeit goods confiscated by U.S. law enforcement agencies in 2013, China hosts vast internal marketplaces — both online and off — where counterfeit goods are traded.[4]

1 Quintanilla, Carl. "War on Counterfeit Goods." CNBC. N.p., n.d. Web. 14 June 2013.

2 United Nations Office on Drugs and Crime. "Transnational Organized Crime: Let's Put Them Out of Business." Counterfeit Goods: A Bargain or a Costly Mistake? N.p., n.d. Web. 29 May 2014.

3 CNN. "Fake Golf Clubs Scam 'Duped' eBay Customers." CNN. N.p., n.d. Web. 23 September 2009.

4 United Nations Office on Drugs and Crime. "Transnational Organized Crime: Let's Put Them Out of Business."

About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a Clarivate Analytics flagship brand, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust. For more information, visit markmonitor.com.

About Clarivate Analytics

Clarivate Analytics accelerates the pace of innovation by providing trusted insights and analytics to customers around the world, enabling them to discover, protect and commercialize new ideas faster. Formerly the Intellectual Property and Science business of Thomson Reuters, we own and operate a collection of leading subscription-based services focused on scientific and academic research, patent analytics and regulatory standards, pharmaceutical and biotech intelligence, trademark protection, domain brand protection and intellectual property management. Clarivate Analytics is now an independent company with over 4,000 employees, operating in more than 100 countries and owns well-known brands that include *Web of Science, Cortellis, Thomson Innovation, Derwent World Patents Index, CompuMark, MarkMonitor* and *Techstreet*, among others. For more information, visit clarivate.com.

More than half the Fortune 100 trust MarkMonitor to protect their brands online.
See what we can do for you.

MarkMonitor Inc.
U.S. (800) 745-9229
Europe +44 (0) 207 433 4000
www.markmonitor.com

White Paper

Seven Best Practices for Fighting Counterfeit Sales Online

Executive Summary

Counterfeit sales represent 5 to 7 percent of world merchandise trade today[1]. The damage these sales do to rightful brand owners goes well beyond revenues and profits: numerous reports have suggested that counterfeit and piracy trade supports terrorism, organized crime and other threats to both national security and human rights. Now, the Internet's rapid growth—along with its instant global reach and anonymity—has significantly escalated the situation.

An entire online supply chain, parallel to legitimate distribution channels, has flourished around counterfeit goods. Online B2B exchanges, in addition to eCommerce sites—many promoted via social media and search engines—commonly traffic in counterfeit goods. Fake products acquired on wholesale sites are sold on auction sites, or at flea markets and shops in the physical world.

Deceptive use of proven marketing techniques—paid search ads, search engine optimization, unsolicited email, the use of branded terms in domain names and more—are important parts of this illicit ecosystem, as savvy counterfeiters apply marketing best practices.

Fortunately, brand owners can adopt their own proven best practices to successfully combat online counterfeit sales. Technology exists for identifying and quantifying worldwide online counterfeiting activity—in both promotion and distribution—as it affects a specific brand. Once visible, infringement can be prioritized and attacked. Unlike anti-counterfeiting strategies in the physical world, however, a two-pronged approach is necessary: brand owners must choke off counterfeit sales at both promotional and distribution points.

The battle against online counterfeit sales can be won. With billions in revenues, critical customer loyalty, and even public safety and human rights at stake, it must.

MarkMonitor®

Contents

Counterfeiting: A Growing Online Threat

"If you can make it, you can fake it." Unfortunately, the old saying is all too true. Sales of counterfeit goods affect a wide range of industries, from high-margin luxury and technology goods to low-margin consumer goods like batteries, shampoo, gasoline and food.

The problem is growing, in part because the volume of fake goods produced is rapidly increasing—especially in countries like China, where manufacturing capacities continue to skyrocket (89 percent of seized counterfeit products originate there).[2]

This growth in supply helps fuel the exploding demand—especially online. The Internet's rapid growth—along with its instant global reach and anonymity—has significantly escalated the situation, moving the sale of counterfeit goods from the local street corner to a global marketplace. Because criminals can quickly and easily set up eCommerce storefronts or place listings on B2B exchanges and on auction sites—with only minor expense—their activities will likely cost legitimate businesses $135 billion in lost revenue this year.

Counterfeiting's Real Cost to Business

According to the secretary general of the ICC, multinational manufacturers lose roughly ten percent of their top-line revenue to counterfeiters[3] —but the impacts go well beyond the revenue hit. For some companies, perceived brand value suffers when knock-offs become plentiful. Brands may even lose representation in distribution channels when resellers and affiliates see a reduction in demand due to competition from fakes. Additionally, the availability of cheaper, albeit fake alternatives can exert downward pressure on legitimate brand pricing.

Other impacts include product safety issues—especially in pharmaceutical, automotive, aviation, healthcare electronics and similar industries—accompanied by increased legal liability risks. And as consumers experience quality problems with fake goods, the legitimate brand's customer service and warranty costs can climb.

Marketing costs also rise as illicit sellers bid up paid search advertising costs and erode legitimate search engine optimization (SEO) investments. Finally, as more customers encounter inauthentic brand experiences, both loyalty and lifetime customer value suffer.

[1] International Chamber of Commerce

[2] *Intellectual Property Rights Seizure Statistics: Fiscal Year 2009*, U.S. Customs & Border Protection, Oct 2009

[3] http://www.livemint.com/2007/06/18001520/Counterfeiters-taking-on-globa.html

How Counterfeiting Thrives Online

Burned by counterfeiters: Zippo Lighters[4]

Revenues: Zippo lost fully one third of its revenues to counterfeiters between 1995 and 2001.

Employment: For every 20,000 fake lighters sold, Zippo reduced staff by 1 full-time employee.

Product Safety: Lower-quality, counterfeit lighters, with a greater tendency to flare up or even explode, caused serious consumer injury.

Liability: Zippo was named in two lawsuits for incidents involving "Zippo lighters" it had not manufactured.

An entire online supply chain—parallel to legitimate distribution channels—has grown around counterfeit goods. This illicit but highly profitable industry takes advantage of the same online tools, techniques and best practices employed by legitimate brands online.

The contrasts with counterfeiting in the physical world are important to understand, and are founded on the Internet's global reach, anonymity, and efficiency. These attributes—and especially the online world's powerful promotional potential—have enabled online counterfeiters to dramatically (and rapidly) outstrip all the street corner fakes, flea markets and "canal street districts" that exist.

In the wholesale trade, B2B exchanges (also known as trade boards) commonly traffic in counterfeit goods. At the retail level, auction sites and eCommerce sites supply counterfeit goods to consumers. It's not unusual for individuals to acquire fake goods on wholesale sites, only to resell them to consumers on auction sites and in other online, consumer-facing venues—in addition to offline flea markets, bazaars, and even retail shops.

Promotion is an important part of this illicit ecosystem. Counterfeiters use the same tactics as legitimate marketers, such as paid search ads and search engine optimization to lure buyers to their sites. According to *Direct Magazine*, fully 14 percent of searches on a branded item lead online users somewhere other than the legitimate brand's site: While some of these searches may lead to legitimate resellers or partners, it's reasonable to assume that many of them end up on the site of a counterfeiter.

Some counterfeit sellers also employ unsolicited email—spam—to boost their site traffic. This is especially prevalent among sellers of fake pharmaceuticals, software, and luxury goods such as watches, jewelry, and high-end apparel. They also make use of cybersquatting techniques, using branded terms in domain names in order to attract web traffic and convey authenticity. And, as savvy marketers, they take advantage of inbound linking strategies and other search engine optimization (SEO) techniques to sell their illicit goods online.

[4] http://www.zippo.com/NewsAndEvents/Counterfeiting_of_Zippo_lighters_In_China_affecting_Bradford.aspx?article=9209ee4c-ff1e-4712-b340-7124bf485164&bncp=1

The counterfeiting ecosystem extends to popular auction and exchange sites, of course, where direct searches frequently include counterfeit goods among their results. Links to sites pushing counterfeit wares can also be found in quantity on social media venues such as social networking sites, blogs and micro-blogs.

Clearly, legitimate and counterfeit ecosystems overlap—with some auction and eCommerce sites selling both real and fake goods—and this makes the problem more difficult to address. There are best practices, however, which can help brands minimize the damage from online counterfeit sales.

Beating Back Counterfeiters Online: Seven Best Practices

While the sale of counterfeit goods in the physical world is a timeworn tradition—if an unwelcome one—the online counterfeiting ecosystem offers unique challenges that require a unique online approach. Proven best practices have emerged from brands that have actively and successfully engaged in combating counterfeit sales online.

1. Attain global visibility. Before a brand can understand the scope of the threat posed by online counterfeit sales, it must expose and quantify the problem. As we have seen, counterfeiters operate over a wide array of online channels; all of these, including B2B exchanges, auction sites, eCommerce sites, message boards, and the rest, must be monitored and analyzed. There's some good news: just ten online marketplaces account for fully 80 percent of all marketplace traffic. Monitor these marketplaces, and you're watching a significant share of traffic.

The counterfeit sales volumes involved cited here—along with everything else about the Internet—are all enabled by technology. The only possible way to approach the monitoring challenge is to leverage technology as well; there is simply no other practical method.

2. Monitor points of promotion. While it's obviously important to identify and shut down distribution channels, it's almost certain that counterfeiters will regularly seek new sales venues. So it's just as critical to monitor the online promotional activities these criminals launch.

Counterfeiters use the same effective promotion techniques employed by legitimate marketers—leveraging the powerful, highly recognizable brands built by experts. Using paid search advertising, links within social media, black hat SEO tactics, cybersquatting and spam, they successfully steer traffic to their illicit offerings, while diminishing the marketing ROI of legitimate brand holders.

Monitoring for these promotional efforts is critical—and enables our next best practice.

The best tools for fighting technology-enabled counterfeit sales.

Brand:	Snap-on Tools
Challenge:	Significant online sales of counterfeit Snap-on tools, resulted in erosion of revenues, perceived brand value, and customer loyalty.
Response:	Snap-on employed sophisticated monitoring and detection technology solutions to fight online counterfeit sales.
Results:	Counterfeit products valued at $1.2 million—found in 4,900 illegal auction listings—were identified and removed in coordination with an online auction site.

3. Take proactive action. Counterfeiters obviously encounter more success when left to operate unchallenged; they're also known to shift their energies to more passive targets when brands visibly fight back. Once a brand understands where the greatest threats lie, aggressive action is the best strategy. Brands should:

- **Set priorities.** The biggest offenders, offering the greatest number of counterfeit goods in the most highly trafficked venues, should be identified and addressed first. Brand owners should determine which counterfeit goods are generating the largest sales, and target them first as well.
- **Watch for cybersquatters.** Brands should actively monitor cyberspace for unauthorized use of their branded terms in domain names. This will aid in rapid detection of eCommerce sites selling counterfeit or unauthorized goods—and frequently also uncovers other abuses such as false association with offensive content like pornography.
- **Become a difficult target.** Brands that visibly, vigorously fight to remove counterfeit goods from online venues often see a dramatic drop in infringement against their brands.
- **Use all your weapons.** Most online channels provide mechanisms for dealing with counterfeit sales situations. Online marketplaces, for example, typically have policies and procedures enabling brand owners to report listings that infringe their brand. Others often respond readily to emailed complaints from brand owners.

  Search engines offer similar facilities. Major search engines have procedures for requesting the removal of ads linked to counterfeit sites. Websites can also be removed from search results pages if they are found to violate copyright laws (a common practice among counterfeit sites, typically through unauthorized use of product images).

  Another useful tactic is the sending of takedown notices, which can be sent directly to Internet service providers. In one recent court case[5], two web-hosting companies were fined $32 million for not responding to takedown notices aimed at blocking counterfeit sales on sites they hosted.
- **Get help from friends.** Industry relationships can be powerful weapons in the fight against online counterfeiting. When choosing a brand protection solution provider, look for one with established ties with thousands of ISPs

[5] Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al. ; http://www.ft.com/cms/s/0/54c5a3a4-9686-11de-84d1-00144feabdc0.html?catid=57&SID=google&nclick_check=1

and registrars worldwide. Simply put, these ties make it possible to get counterfeit sites shut down more quickly—and thereby minimize brand owner losses. Trade associations such as the International AntiCounterfeiting Coalition (IACC), the Anti-Counterfeiting Group (ACG) and the American Apparel and Footwear Association (AAFA) also provide resources and advice on best practices for fighting counterfeiters.

4. Fight online counterfeit sales holistically. Online counterfeit sales are easier to address when the entire enterprise participates. That means brand owners should set up a cross-functional task force to address the issue in a coordinated, holistic manner.

Stakeholders—and, therefore, recommended participants—will vary by industry and enterprise, but can include legal, marketing, risk management, loss prevention, channel sales management, manufacturing, supply chain management, and other functional units.

Because fighting online counterfeiting requires attacking both promotional mechanisms and distribution channels, this group will be larger than needed to fight physical-world counterfeiting. All of these groups can and should set priorities and strategy for detecting, reporting and responding to infringers—both online and off— and should continue to inform the process as their situations and perceptions dictate.

5. Let online intelligence inform offline defense measures. Because offline measures—physical investigations, factory raids and other activities—can be costly and time-consuming, it's critical to know where they should be focused. Online intelligence can help identify the most egregious infringers, so that offline defensive efforts can be focused where they'll be most effective.

6. Act swiftly—and globally. Perhaps even more than it affects legitimate business, the proliferation of international trade offers tremendous benefits to online counterfeiters. While a domestic seller or manufacturer may seem like an easy first target, brands have learned that it's more effective to launch global anti-counterfeiting initiatives—and to get them underway expeditiously.

Footwear manufacturer stomps online counterfeiters.

Global footwear leader Deckers Outdoor, faced with millions in online sales of counterfeit and grey market goods, moved promptly to protect its customers and its bottom line. Leveraging brand protection technology, the company was able to:

- Pinpoint—and remove or de-list—$4.35 million in illegitimate goods and knock-offs, all within just 90 days
- Significantly curtail counterfeiting activity that undermined its revenues
- Enhance its brand reputation and increase customer trust and loyalty by automating and extending online enforcement

Online intelligence helps focus physical efforts.

Acushnet Company, a leader in the golf industry, leveraged online intelligence to guide a major raid in the UK, shutting down a large counterfeiting operation that fed online distribution channels.[6]

[6] CNN: http://edition.cnn.com/2009/SPORT/09/23/golf.ebay.clubs.scam

Prepare by ensuring your trademarks are registered internationally—especially in China, which observes a "first-to-file" policy that grants registration to whoever files first, even if it's not the true brand owner.

Global imaging giant protects its image—and profits.

Print technology leader Epson created a centralized mechanism for globally monitoring for online brand abuses including counterfeit sales.

By forming a global, cross-functional team, Epson achieved a three-fold reduction in counterfeit sales activities on consumer auction and B2B exchange sites. Their visible, aggressive strategy has also served to deter abuse.

Tall order: fighting counterfeiting in China.

One of the most important centers of counterfeit trade is China. In addition to originating roughly 89% of counterfeit manufactured goods, China hosts vast internal marketplaces—both online and off—where counterfeit goods are traded.

A global effort doesn't preclude addressing markets that are internal to a given country. In some cases, this will require competent language translation resources for monitoring, detection and enforcement. Most companies rely on third-party brand protection solution providers for this kind of expertise.

Many online B2B exchanges and auctions are presented only in Chinese-language characters, posing translation barriers to legitimate brands aiming to protect their rights. Regardless of the source of counterfeit goods sold on these sites, buyers commonly re-sell the illicit products in other online and offline venues. Losses to legitimate brands are in the billions.

7. Educate your customers. Your customers can be an important ally in minimizing sales of counterfeit goods with all its associated costs. Work aggressively to show customers the risks of buying from unauthorized sources, and recruit them to join in the effort by reporting suspicious goods and sellers.

Many brands have established web-based tools for verifying the authenticity of goods and/or the legitimacy of sellers. Others provide form- or email-based mechanisms for reporting suspected infringement. When offering such tools, be sure to reinforce the benefits of buying authentic goods from authorized sellers.

Another effective, pro-active measure enables brands to warn consumers directly of known counterfeiting activity, before the consumer makes a purchase. This patented technology leverages relationships with major Internet security providers to deliver early warnings to Internet users, waving them off before they click through to a site known to traffic in counterfeit or recalled goods.

Many consumers don't want cheap knock-offs—and they don't want their authentic goods cheapened by the presence of illicit goods. Take advantage of these sentiments: join forces with your customers to spot counterfeit products quickly and help get them off the market.

Conclusion: The Fight Is Yours to Win

Online counterfeiting can heavily impact any company, affecting revenues, channel relationships, customer experience, marketing effectiveness, legal liability and more. Ignoring it—or just hoping for the best—simply isn't good business.

Fortunately, taking action can be fairly straightforward. Implementing the best practices discussed here doesn't have to involve complex organizational changes or extensive hiring efforts, as third-party solution providers can help make the effort efficient and supplement internal teams.

To successfully reduce the negative effects of counterfeiting, however, companies must commit to forming a cross-functional team, at least at the advisory level, and to an aggressive, global anti-counterfeiting initiative.

Most importantly: to effectively choke off counterfeit sales, these teams must ensure a strategy that focuses on both distribution and promotional mechanisms associated with counterfeit goods. The returns—in revenues, profits, and long-term brand value—will certainly make the effort worthwhile.

About MarkMonitor

As the global leader in online brand protection, MarkMonitor provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of industry-leading expertise, advanced technology and extensive industry relationships to preserve their marketing investments, revenues and customer trust.

To learn more about MarkMonitor, our solutions and services, please visit **markmonitor.com** or call us at **1-800-745-9229**.

More than half the Fortune 100 trust MarkMonitor to protect their brands online. **See what we can do for you.**

MarkMonitor, Inc.
U.S. (800) 745.9229
Europe +44 (0) 203.206.2220
www.markmonitor.com

EXHIBIT 2

Intellectual Property Rights Seizure Statistics

U.S. Customs and Border Protection

Fiscal Year 2020

CONTENTS

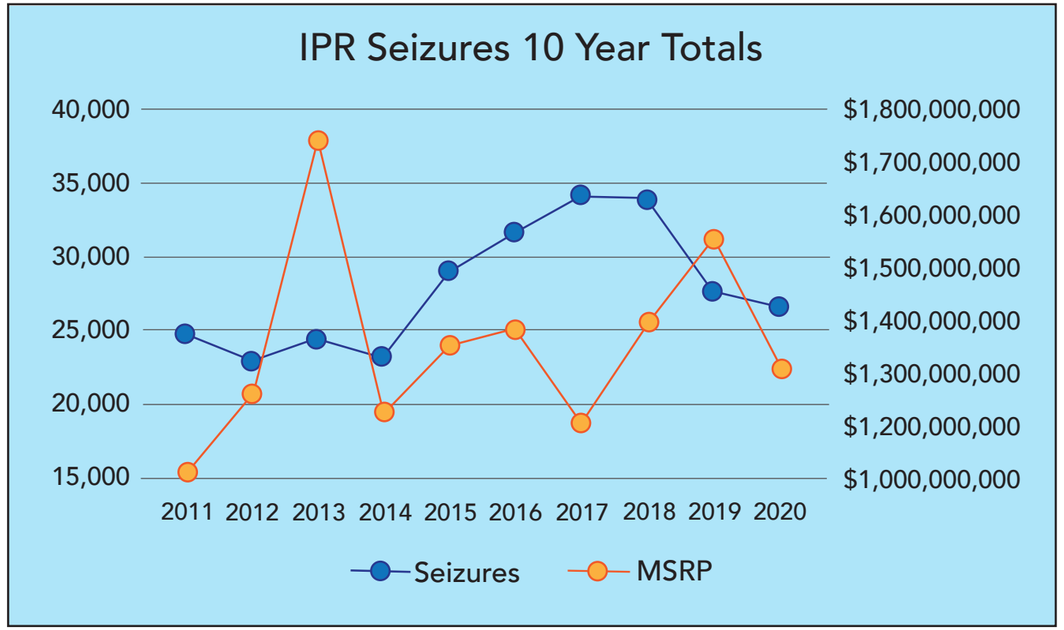
Disclaimer: The information contained in this report does not constitute the official trade statistics of the United States. The statistics, and the projections based upon those statistics, are not intended to be used for economic analysis, and are provided for the purpose of establishing U.S. Department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

Executive Summary

U.S. Customs and Border Protection focuses its trade enforcement efforts on seven Priority Trade Issues (PTI). PTIs represent high-risk areas that can cause significant revenue loss, harm the U.S. economy, or threaten the health and safety of the American people. Current PTIs include **Intellectual Property Rights (IPR)**, which protect American Intellectual Property by interdicting violative goods and leveraging enhanced enforcement authorities.

Trade in illegitimate goods is associated with smuggling and other criminal activities, and often funds criminal enterprises. CBP protects the intellectual property rights of American businesses, safeguarding them from unfair competition and use for malicious intent while upholding American innovation and ingenuity. CBP works with many partner government agencies and the trade community to mitigate the risks posed by imports of such illicit goods.

FY 2020 was another successful year for IPR enforcement. CBP made **26,503 seizures** with an estimated manufacturer's suggested retail price (MSRP) of over **$1.3 billion**.



COVID-19 Spotlight

In FY 2020, CBP saw a shift in certain product category seizures, including counterfeit, unapproved, or otherwise substandard COVID-19 related products that threatened the health and safety of American consumers, including the following:

COVID-19 Related Seizures FY 2020

Product	# of incidents	# of items seized
Counterfeit face masks	352	12.7 million
Prohibited COVID-19 test kits	378	180,000
Prohibited Chloroquine tablets	221	38,000

Over half of these seizures occurred in the express consignment environment and 24 percent were intercepted in international mail. Roughly 51 percent originated in China. In order to curb the sale of counterfeit or substandard COVID-19 sanitation products or safety equipment online, CBP also published the *E-Commerce Consumer Awareness for COVID-19 Safety Guide*: *http://www.cbp.gov/document/guides/e-commerce-consumer-awareness-covid-19*

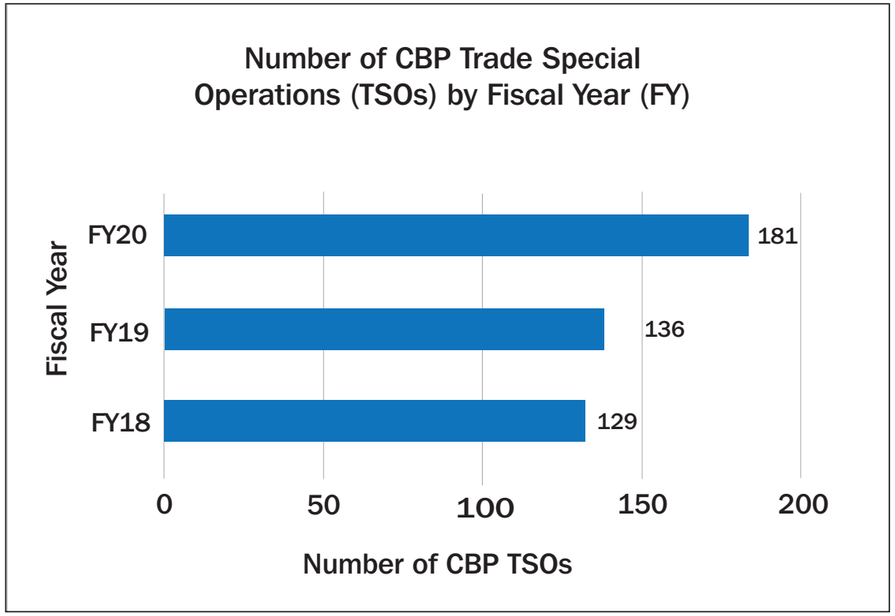
In addition, CBP created the *COVID-19 Cargo Resolution Team* (CCRT), comprised of a network of subject matter experts from across the agency. The CCRT triaged incoming requests from importers and customers; coordinated with federal, state, and local government agencies; facilitated inbound shipments through ports of entry; expedited importation of critical medical supplies; and responded directly to inquiries about the importation of personal protective equipment, COVID-19 test kits, ventilators, and other medical supplies.

In FY 2020, the CCRT responded to 2,611 questions from the trade community and facilitated clearance of 480 Federal Emergency Management Agency-arranged flights, filled with critical medical supplies from legitimate vendors and international donors.

To read more about CBP's efforts during the pandemic, please visit *https://www.cbp.gov/newsroom/coronavirus*.

Operational and Enforcement Highlights

In FY 2020, 70 national level IPR Trade Special Operations (TSOs) and 111 local IPR-TSOs were conducted, representing a total of 181 IPR-TSOs in FY 2020. These TSOs targeted high-risk shipments across the United States and resulted in 219 seizures of IPR-infringing goods which, if genuine, would have an estimated MSRP of $1.7 million. This represents a 104% increase in MSRP from IPR-trade special operations from FY 2019.



CBP Partnerships

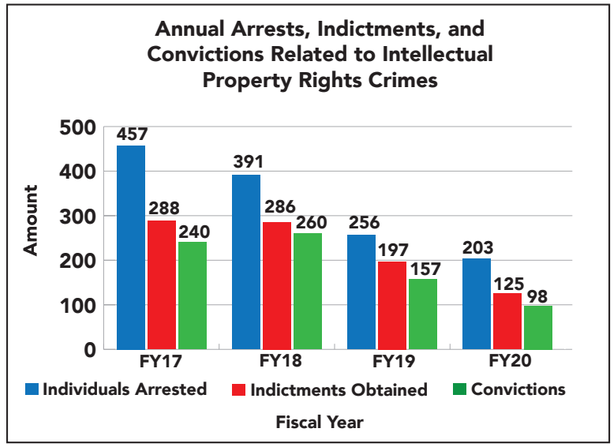
CBP works with partner government agencies to facilitate legitimate trade that supports economic growth and shields the American public and businesses from unsafe products, intellectual property theft, and unfair trade practices.

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

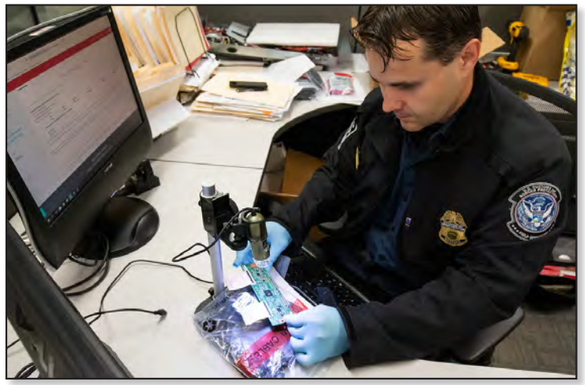
CBP and ICE-HSI mitigate the welfare and financial risks posed by imports of illicit products. In FY20, ICE-HSI arrested 203 individuals, obtained 125 indictments, and received 98 convictions related to intellectual property crimes.

Collaboration Spotlight: In partnership with CBP, HSI launched *Operation Stolen Promise* (OSP) in April 2020 to protect the Homeland from the increasing and evolving threat posed by COVID-19-related fraud and criminal activity. As part of OSP, CBP Officers and HSI special agents have opened investigations nationwide, seized millions of dollars in illicit proceeds; made multiple arrests; and shut down thousands of fraudulent websites.

HSI continues to work alongside CBP to seize shipments of mislabeled, fraudulent, unauthorized, or prohibited COVID-19 test kits, treatment kits, homeopathic remedies, and purported anti-viral products and personal protective equipment (PPE).



Operation Stolen Promise 2.0 has been launched to expand the focus of OSP to address the emerging public health threat of counterfeit versions of COVID-19 vaccines and treatments entering the marketplace.



CBP Partnerships

The United States Postal Service (USPS)
USPS is responsible for presenting mail and providing electronic data (AED) to CBP for arriving international mail parcels. USPS and CBP have worked to target and identify 31 violations imported through international mail. Both agencies are implementing new strategies for leveraging the AED already available to identify offending merchandise.

Collaboration Spotlight: *Operation Mega Flex* is a CBP-led, interagency effort that was initiated in July 2019 to measure compliance and assess illicit networks in the international mail environment through periodic enhanced inspections. CBP conducts Mega Flex operations at international mail facilities and express consignment hubs nationwide in close coordination with ICE and the USPS.

Through *Operation Mega Flex*, CBP has found that more than 13 percent of targeted shipments contain counterfeit goods or contraband. Since July 2019, CBP has seized more than 4,800 shipments and nearly 2,600 agriculture violations through Mega Flex that posed health, safety, or economic threats to the United States and its people.

To read more about CBP's specific *Operation Mega Flex* efforts, visit *CBP New York Field Office Seizes 127 IPR Violations During Operation Mega Flex* and *XVI Operation Mega Flex Stops Hundreds of Illicit "Made in China" Shipments at LAX*: https://www.cbp.gov/newsroom/local-media-release/cbp-new-york-field-office-seizes-127-ipr-violations-during-operation and https://www.cbp.gov/newsroom/local-media-release/operation-mega-flex-stops-hundreds-illicit-made-china-shipments-lax

The National Intellectual Property Rights Coordination Center (IPR Center)

The IPR Center, in collaboration with CBP, stands at the forefront of the United States government's response to combatting global intellectual property (IP) theft and enforcement of its international trade laws.

Collaboration Spotlight: *Operation Team Player* is an ongoing annual operation that begins after every Super Bowl and continues through the next one, targeting international shipments of counterfeit sports merchandise into the United States. This operation is run by the IPR Center in collaboration with CBP, the NFL, and other major sports leagues to prevent the illegal importation and distribution of counterfeit sports merchandise.

Super Bowl LIV was played on February 2, 2020 at Hard Rock Stadium in Miami Gardens, Florida. U.S. CBP and ICE HSI announced the seizure of more than 176,000 counterfeit sports-related items, worth an estimated $123 million manufacturer's suggested retail price (MSRP), through a collaborative enforcement operation targeting international shipments of counterfeit merchandise into the United States.

CBP Partnerships

Commercial Customs Operations Advisory Committee (COAC)
The private sector plays an instrumental role in the global economy and has a unique opportunity to lend their considerable expertise to CBP. By partnering with industry leaders, CBP links our processes with modern business practices, which results in enhanced compliance with trade laws, improves our facilitation and enforcement efforts, and assists the U.S. economy. CBP's engagement with its federal advisory committee, the COAC, is a key component in evaluating and adapting CBP policies and getting feedback about significant proposed changes.

In September 2020, CBP developed a new Statement of Work (SOW) to re-engage the COAC Intellectual Property Rights Working Group (IPRWG). The SOW requested the IPRWG to further develop, expand upon, and align three previous recommendations pertaining to sharing of detention information, photographic standards guide, and data-driven CBP seizure process. We look forward to continued progress with the upcoming 16th term of COAC.

Public Awareness Campaign: "The Truth Behind Counterfeits"
In FY 2020, CBP continued *"The Truth Behind Counterfeits"* https://www.cbp.gov/trade/fakegoodsrealdangers. IPR public-awareness campaign to educate the public about the potential harm of counterfeit goods by making people aware that buying counterfeits is not a victimless crime and encouraging them to shop from well-known and reputable sources. The campaign ran at major U.S. airports including NYC, Charlotte, Minneapolis, Denver, Miami, Pittsburgh, and Baltimore during the busy 2019 holiday and travel season.

In addition to the large ads that were displayed at the airports, the campaign also included a digital component that targeted ads online in these same cities. The campaign and its messages about responsible consumer behavior were viewed an estimated 106 million times throughout the period from Thanksgiving through the New Year.

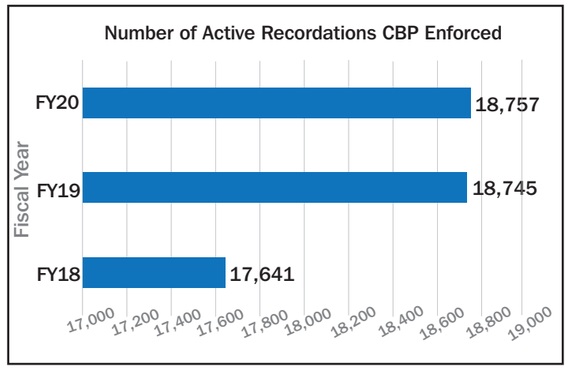
Help CBP Protect American Ingenuity

Donations Acceptance Program
As part of TFTEA, CBP prescribed regulations (19 CFR 133.61) for receiving donations from private sector parties of hardware, software, equipment, and technologies for the purpose of enforcing IPR. Administered through CBP's *Donations Acceptance Program* (DAP), this program has yielded several high-profile public-private partnerships that have already demonstrably enhanced CBP's ability to more quickly and accurately detect counterfeit merchandise entering the U.S. In FY 2020, Cisco donated additional barcode scanners raising the total number of tools being used to 16 in conjunction with their online package look-up tool which are now impacting six CBP Field Offices. Since the regulation went into effect in January 2018, the DAP has fully executed four formal IPR enforcement partnerships and is in process of completing one more with Nike, Inc. in FY 2021.

Intellectual Property Rights e-Recordation
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, *https://iprr.cbp.gov/*. CBP administers these recordations using a secure proprietary database. Product ID manuals provided by rights holders are also linked to the database and used by CBP in making IPR border enforcement determinations.

Intellectual Property Rights Search
CBP works closely with rights holders in making IPR enforcement determinations. A public database of both active and inactive recordations is available using a search engine called the Intellectual Property Rights Search (IPRS) at *http://iprs.cbp.gov/* Information on potential IPR infringements can be submitted to CBP using the e-Allegations Online Trade Violation Reporting System at *https://eallegations.cbp.gov/Home/Index2*.

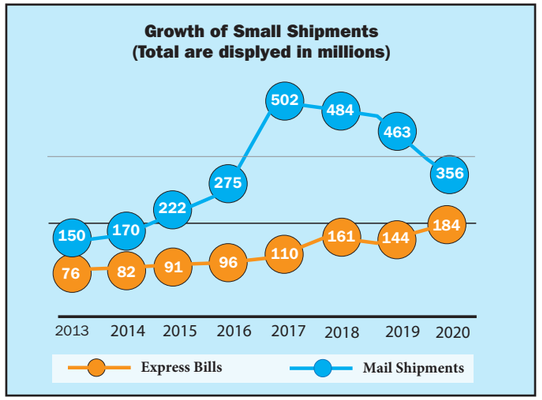
As of September 30, 2020, CBP was enforcing **18,757 active recorded copyrights and trademarks**. In FY 2020, CBP's Office of Trade (OT) received and responded to **455 inquiries** from the field concerning IPR enforcement. This represents a 20 percent increase from FY 2019. At the end of FY 2020, CBP was administering **127 active exclusion orders** issued by the U.S. International Trade Commission (USITC) following investigations of unfair import practices in the importation of articles into the U.S. in violation of 19 U.S.C. § 1337, the majority of which are based on allegations of patent infringement. CBP's enforcement of these orders resulted in **137 exclusion order administrative actions**.



IPR & E-Commerce

E-Commerce sales have contributed to large volumes of low-value packages imported into the United States. In FY 2020, there were 184 million express shipments and 356 million international mail shipments. Many of these shipments contain counterfeit goods that pose the same health, safety, and economic security risks as containerized shipments. Over 90 percent of all intellectual property seizures occur in the international mail and express environments. The ongoing e-commerce revolution drove a 28 percent increase in low-value shipments and a 219 percent increase in air cargo in Fiscal Year 2020.

In response to the increase in e-commerce, CBP has created a modernized enforcement and facilitation framework for e-commerce through the administration of Section 321 Data Pilot and Entry Type 86 Test.



Section 321 Data Pilot
Initiated in 2019, the Section 321 Data Pilot is a voluntary collaboration with online marketplaces, carriers, technology firms, and logistics providers to secure e-commerce supply chains and protect American consumers. The pilot allows CBP to accept shipment-level information directly from online marketplaces and match it with the information received from traditional carriers. As a result, CBP is empowered to better segment risk and to perform more effective and efficient targeted screening with respect to Section 321 shipments. The number of shipments qualifying for the Section 321 exemption has greatly increased, largely due to the enactment of TFTEA, which raised the de minimis value cap from $200 to $800.

Entry Type 86
The Entry Type 86 Test provides filing capabilities through the Automated Broker Interface, accommodates entries that include PGA data and the 10-digit Harmonized Tariff Schedule, and expedites clearance of compliant de minimis shipments into the United States.

The pilots have shown significant operational and private sector benefits when seller, enhanced product description and other transactional details are provided. Combined, CBP has received enhanced targeting and admissibility data on over 300 million shipments to date.

CBP is also working to educate the public, including consumers and importers alike, of the risks associated with non-compliant products. In FY 2020, CBP published the *E-Commerce Counterfeit Awareness Guide for Consumers* and the *E-Commerce Counterfeit Awareness Guide* for Importers to create awareness for consumers and importers about their responsibilities to comply with customs regulations. Additionally, CBP issued an administrative ruling clarifying the duty-free status of certain low-value shipments. Visit https://www.cbp.gov/trade/basic-import-export/e-commerce to learn more about CBP's efforts in e-commerce.

Exclusion Orders

CBP enforces exclusion orders issued by the International Trade Commission (ITC). Most ITC exclusion orders are patent-based. The ITC issues both limited and general exclusion orders. Limited exclusion orders apply only to infringing articles of named respondents. General exclusion orders bar the entry of infringing articles by all.

Exclusion orders prohibit the entry of all covered articles, even if they were not specifically accused and found to infringe by the ITC. Once excluded, subsequent importations of the same articles by the same importer are subject to seizure.

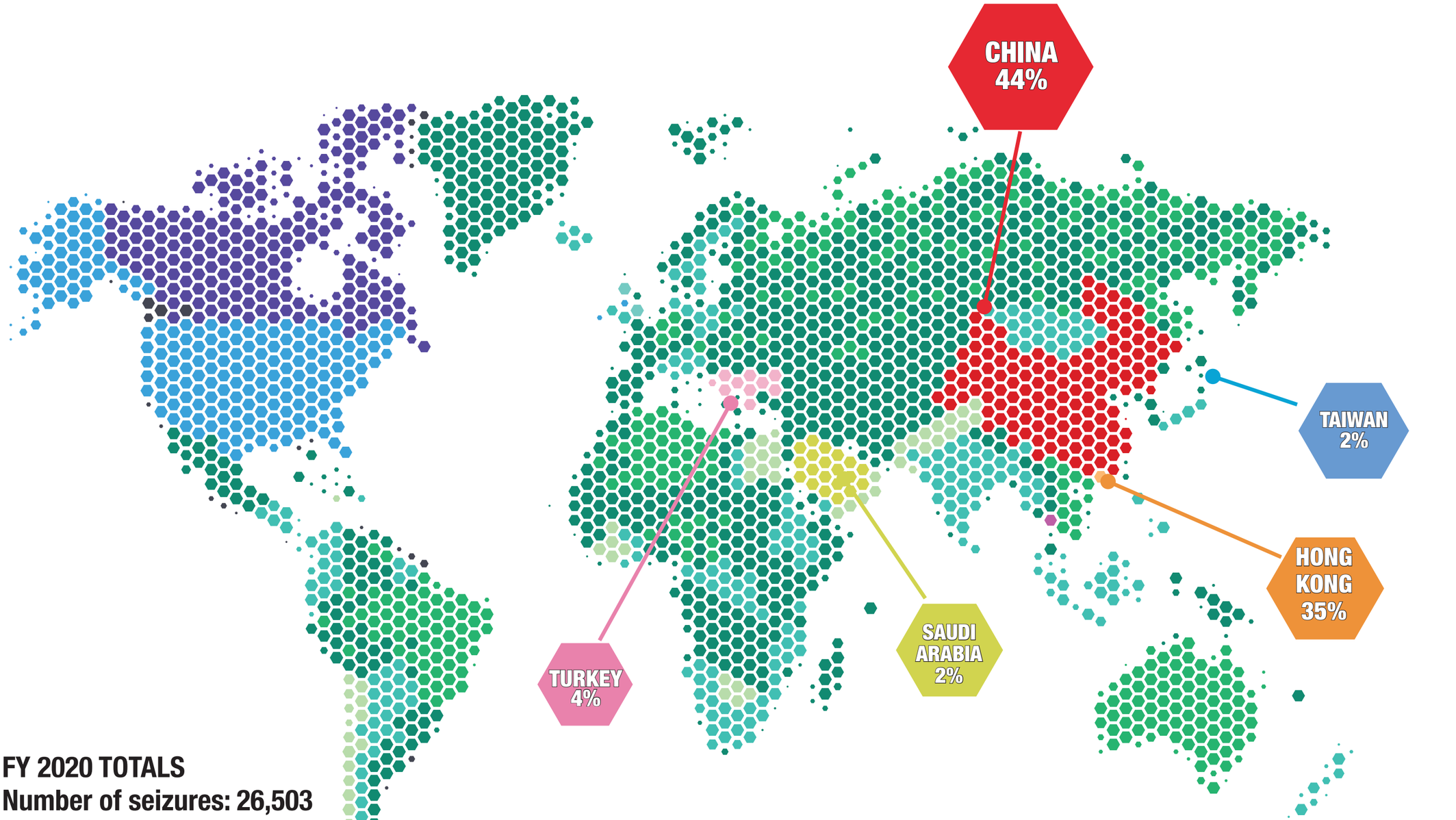
Fiscal Year 2020			
Shipments Seized	Seizure Est. MSRP	New Exclusion Orders Issued	Total Active Exclusion Orders
169	$12,241,036	24	128*

Notes:
For shipments seized under an active exclusion order, in FY20 a total of 169 seizures cited 19 USC 1337(i) with a total MSRP of $12,241,036. During FY 2020, CBP enforced up to 128 active exclusion orders.
*The term "rulings" covers rulings and other interpretive decisions.**

Modes of Transportation and Commodities

Fiscal Year 2020 IPR Seizures Statistics
By Number Of Seizures

Seizure World Map

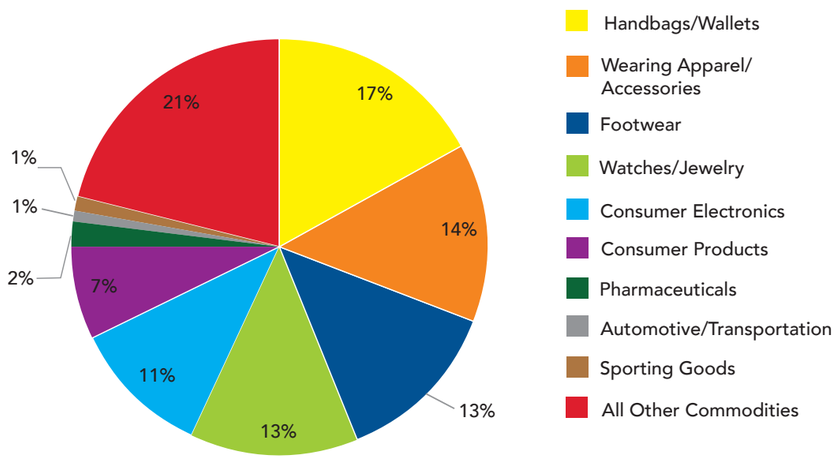


FY 2020 TOTALS
Number of seizures: 26,503
MSRP: $1.3 billion

ALL OTHER COUNTRIES 13%

Number of Seizures

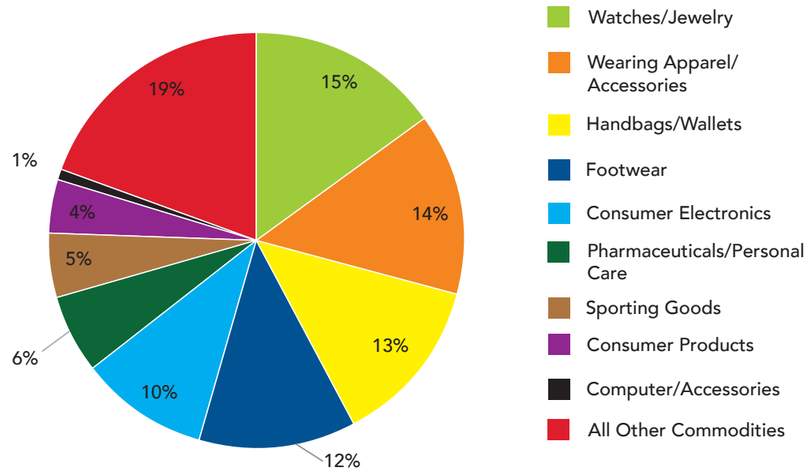
Fiscal Year 2020



2020		
Products	**Seizures**	**% of Total***
Handbags/Wallets	4,597	17%
Wearing Apparel/Accessories	3,592	14%
Footwear	3,460	13%
Watches/Jewelry	3,460	13%
Consumer Electronics	3,024	11%
Consumer Products	1,932	7%
Pharmaceuticals	495	2%
Automotive/Transportation	299	1%
Sporting Goods	206	1%
All Other Commodities	5,438	21%
Number of Seizures	**26,503**	**100%**

Number of Seizures: 26,503

Fiscal Year 2019



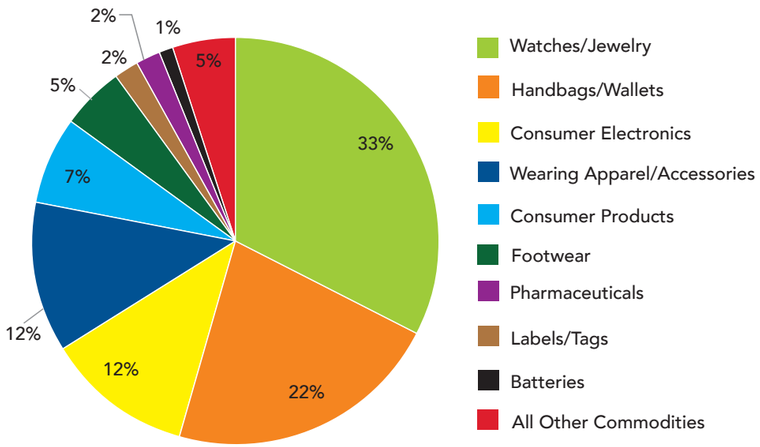
Number of Seizures: 27,599

2019		
Products	**Seizures**	**% of Total***
Watches/Jewelry	4,242	15%
Wearing Apparel/Accessories	3,841	14%
Handbags/Wallets	3,653	13%
Footwear	3,249	12%
Consumer Electronics	2,681	10%
Pharmaceuticals/Personal Care	1,779	6%
Sporting Goods	1,510	5%
Consumer Products	1,219	4%
Computers/Accessories	318	1%
All Other Commodities	5,107	19%
Number of Seizures	**27,599**	**100%**

**Seizures involving multiple product categories are included in the "All Others" category. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100 percent.*

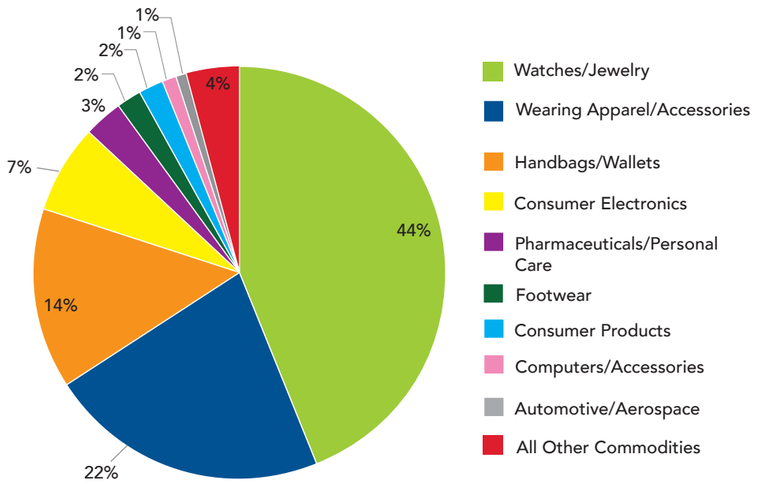
Products Seized by MSRP

MSRP FY 2020



Total FY 2020 MSRP $1,309,156,510

MSRP FY 2019



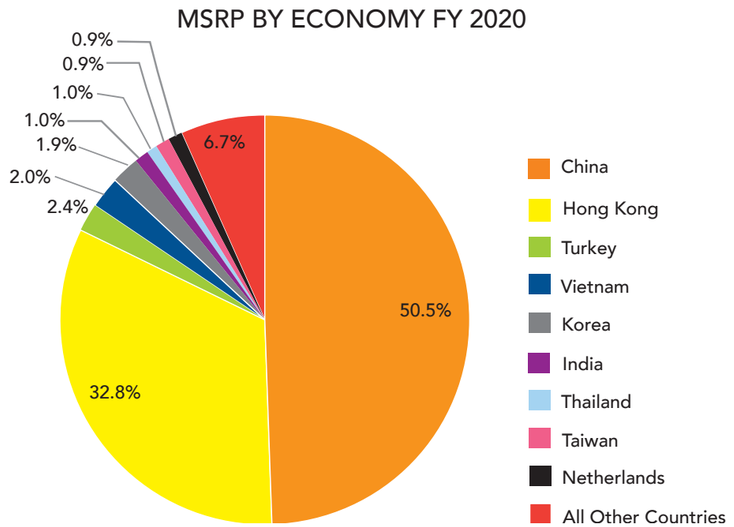
Total FY 2019 MSRP $1,555,269,057

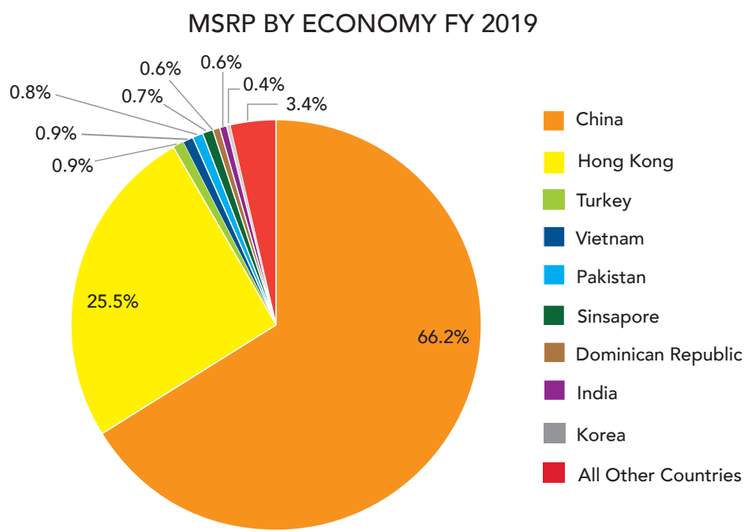
FY 2020		
Products	**MSRP**	**% of Total***
Watches/Jewelry	$ 435,249,467	33%
Handbags/Wallets	$ 282,702,448	22%
Consumer Electronics	$ 162,234,924	12%
Wearing Apparel/Accessories	$ 157,226,661	12%
Consumer Products	$ 85,470,866	7%
Footwear	$ 63,146,456	5%
Pharmaceuticals	$ 20,414,897	2%
Labels/Tags	$ 19,823,791	2%
Batteries	$ 14,432,379	1%
All Other Commodities	$ 68,454,621	5%
Total FY 2020 MSRP	**$ 1,309,156,510**	**100%**
Number of Seizures	**26,503**	**100%**

FY 2019		
Products	**MSRP**	**% of Total***
Watches/Jewelry	$ 687,167,057	44%
Wearing Apparel/Accessories	$ 343,732,063	22%
Handbags/Wallets	$ 212,781,760	14%
Consumer Electronics	$ 105,957,198	7%
Pharmaceuticals/Personal Care	$ 48,771,870	3%
Footwear	$ 37,994,046	2%
Consumer Products	$ 27,907,721	2%
Computers/Accessories	$ 13,216,628	1%
Automotive/Aerospace	$ 12,142,621	1%
All Other Commodities	$ 65,598,093	4%
Total FY 2019 MSRP	**$ 1,555,269,057**	**100%**
Number of Seizures	**27,599**	**100%**

**Seizures involving multiple product categories are included in the "All Others" category. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100 percent.*

Total MSRP for Products Seizures by Economy





Total MSRP for Products Seizures by Economy

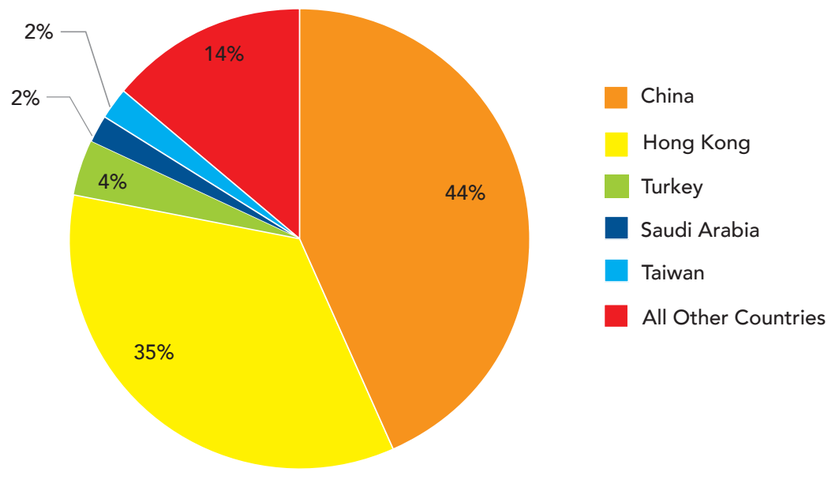
FY 2020		
Trading Partner	**MSRP**	**% of Total***
China	$ 660,767,476	50.5%
Hong Kong	$ 428,961,694	32.8%
Turkey	$ 31,237,035	2.4%
Vietnam	$ 25,803,755	2.0%
Korea	$ 25,282,668	1.9%
India	$ 12,862,390	1.0%
Thailand	$ 12,601,807	1.0%
Taiwan	$ 12,143,980	0.9%
Netherlands	$ 11,796,923	0.9%
All Other Countries	$ 87,698,782	6.7%
Total FY 2020 MSRP	**$ 1,309,156,510**	**100%**
Number of Seizures	**26,503**	

FY 2019		
Trading Partner	**MSRP**	**% of Total***
China	$ 1,030,181,869	66.2%
Hong Kong	$ 397,276,566	25.5%
Turkey	$ 14,240,890	0.9%
Vietnam	$ 13,556,034	0.9%
Pakistan	$ 12,157,097	0.8%
Singapore	$ 10,452,581	0.7%
Dominican Republic	$ 9,542,456	0.6%
India	$ 9,539,580	0.6%
Korea	$ 5,633,115	0.4%
All Other Countries	$ 52,688,870	3.4%
Total FY 2019 MSRP	**$ 1,555,269,057**	**100%**
Number of Seizures	**27,599**	

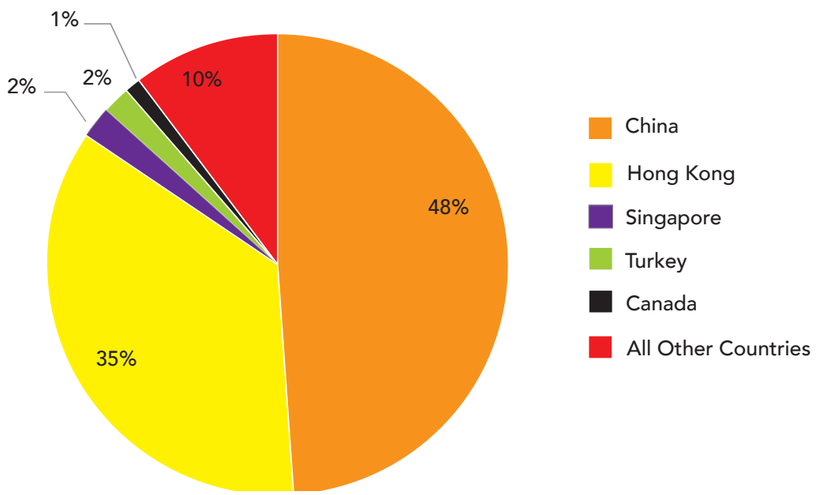
**The aggregate seizure data reflect the reported country of origin, not necessarily where the seized goods were produced. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100 percent.*

Seizures by Economy

SEIZURES BY ECONOMY FY 2020



SEIZURES BY ECONOMY FY 2019



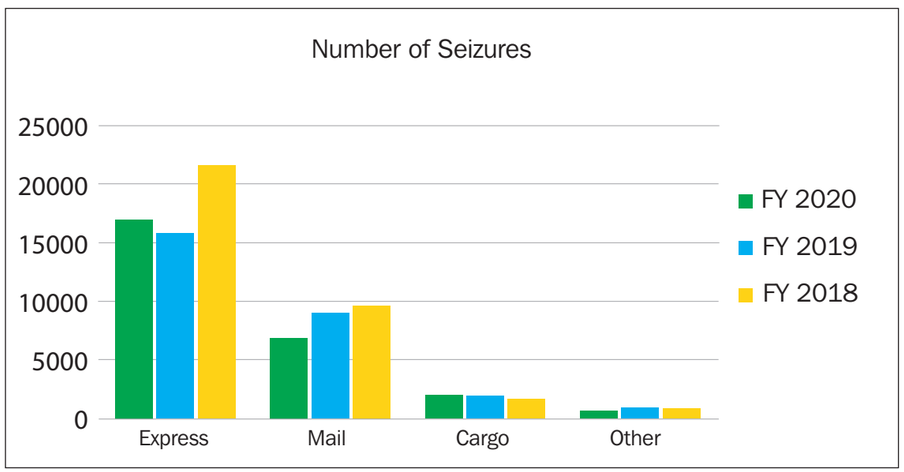
Seizures by Economy

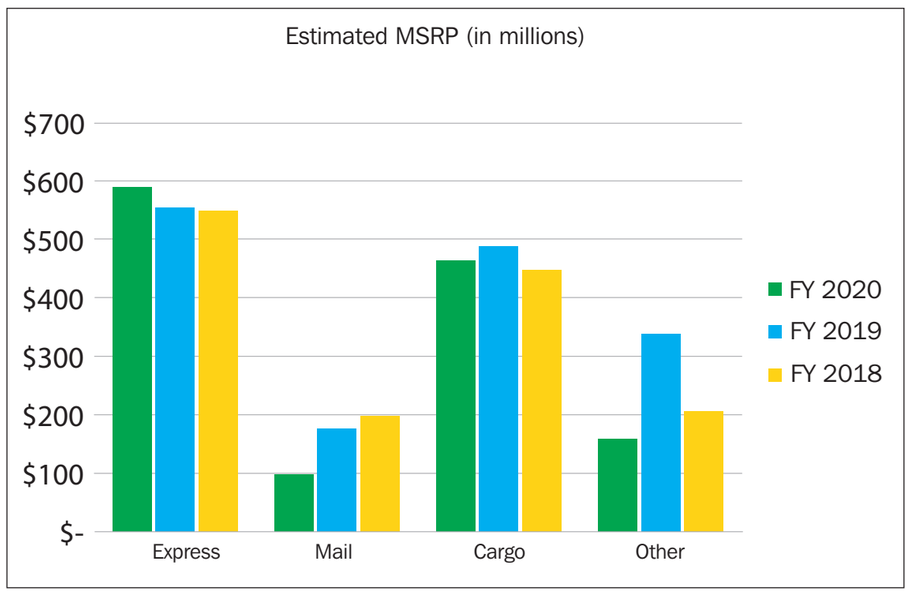
FY 2020		
Trading Partner	**Seizures**	**% of Total***
China	11,710	44%
Hong Kong	9,199	35%
Turkey	1,096	4%
Saudi Arabia	492	2%
Taiwan	423	2%
All Other Countries	3,583	13%
Number of Seizures	**26,503**	**100%**

FY 2019		
Trading Partner	**Seizures**	**% of Total***
China	13,293	48%
Hong Kong	9,778	35%
Singapore	649	2%
Turkey	614	2%
Canada	598	2%
All Other Countries	2,667	10%
Number of Seizures	**27,599**	**100%**

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

Seizures by Mode of Transportation



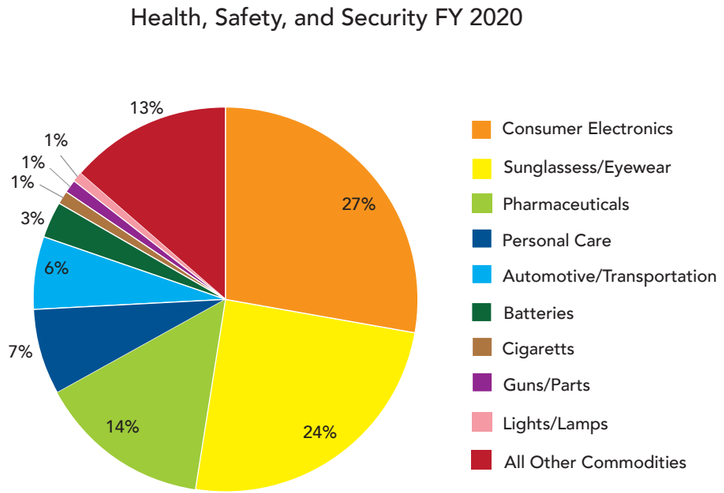


Seizures by Mode of Transportation

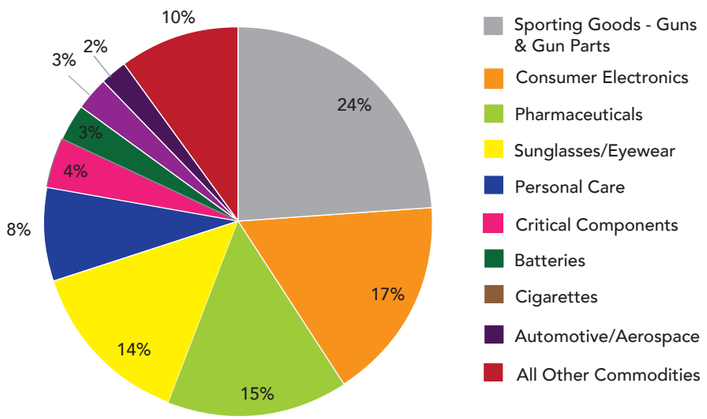
Seizures						
Mode of Transport	FY 2020		FY 2019		FY 2018	
	Seizures	% of Total	Seizures	% of Total	Seizures	% of Total
Express	17,001	64%	15,811	57%	21,632	64%
Mail	6,886	26%	8,982	33%	9,643	29%
Cargo	1,993	8%	1,903	7%	1,673	5%
Other	623	2%	903	3%	862	3%
Total	**26,503**	100%	**27,599**	100%	**33,810**	100%

Estimated Manufacturer's Suggested Retail Price (in millions)						
Mode of Transport	FY 2020		FY 2019		FY 2018	
	MSRP	% of Total	MSRP	% of Total	MSRP	% of Total
Express	$ 589.1	45%	$ 553.3	36%	$ 549.2	39%
Mail	$ 98.1	7%	$ 175.6	11%	$ 197.3	14%
Cargo	$ 463.4	35%	$ 488.2	31%	$ 447.9	32%
Other	$ 158.5	12%	$ 337.9	22%	$ 205.4	15%
Total	**$ 1,309.1**	100%	**$ 1,555.2**	100%	**$ 1,399.8**	100%

Health, Safety, and Security



Number of Seizures: 3,487



Number of Seizures: 5,859

FY 2020		
Health, Safety, and Security	**Seizures**	**% of Total***
Consumer Electronics	944	27%
Sunglasses/Eyewear	844	24%
Pharmaceuticals	501	14%
Personal Care	236	7%
Automotive/Transportation	216	6%
Batteries	88	3%
Cigarettes	82	2%
Guns/Parts	71	2%
Lights/Lamps	58	2%
All Other Commodities	447	13%
Number of Seizures	**3,487**	**100%**

FY 2019		
Health, Safety, and Security	**Seizures**	**% of Total***
Sporting Goods - Guns & Gun Parts	1,428	24%
Consumer Electronics	989	17%
Pharmaceuticals	858	15%
Sunglasses/Eyewear	818	14%
Personal Care	490	8%
Critical Components	216	4%
Batteries	186	3%
Cigarettes	163	3%
Automotive/Aerospace	149	3%
All Other Commodities	562	10%
Number of Seizures	**5,859**	**100%**

**Shipments with multiple types of products are included in the "All others" category. Because the individual percentage figures are rounded, in some cases, the sum of the rounded percentages for a given fiscal year is slightly higher or lower than 100 percent*

Health, Safety, and Security

Seizures and Total MSRP by Centers of Excellence and Expertise

FY 2020		
Centers	**Total MSRP**	**% of Total MSRP**
Consumer Products & Mass Merchandising	$ 841,588,271	64.3%
Apparel, Footwear & Textiles	$ 231,915,396	17.7%
Electronics	$ 170,643,120	13.0%
Machinery	$ 22,860,881	1.7%
Pharmaceuticals, Health & Chemicals	$ 21,024,365	1.6%
Automotive & Aerospace	$ 10,857,996	0.8%
Base Metals	$ 6,111,920	0.5%
Industrial & Manufacturing Materials	$ 3,260,622	0.2%
Agriculture & Prepared Products	$ 893,941	0.1%
Total FY 2020 MSRP	**$ 1,309,156,510**	**100%**

FY 2019		
Centers	**Total MSRP**	**% of Total MSRP**
Consumer Products & Mass Merchandising	$ 1,000,628,016	64.3%
Apparel, Footwear & Textiles	$ 383,694,303	24.7%
Electronics	$ 117,028,274	7.5%
Machinery	$ 27,810,170	1.8%
Pharmaceuticals, Health & Chemicals	$ 9,234,202	0.6%
Automotive & Aerospace	$ 9,868,483	0.6%
Agriculture & Prepared Products	$ 3,882,013	0.2%
Industrial & Manufacturing Materials	$ 1,225,896	0.1%
Base Metals	$ 1,897,700	0.1%
Petroleum, Natural Gas & Minerals	–	0.0%
Total FY 2019 MSRP	**$ 1,555,269,057**	**100%**

IPR Points of Contact

Questions? Contact the IPR Help Desk For Assistance - CBP's IPR Help Desk is staffed Monday through Friday to answer questions on IPR enforcement. Contact the IPR Help Desk via email at IPRHELPDESK@cbp.dhs.gov

Regulations, Rulings, and Recordation – Inquiries about CBP's IPR regulations may be addressed to Regulations and Rulings (RR) at hqiprbranch@cbp.dhs.gov. Ruling requests regarding articles potentially subject to an ITC exclusion order may be submitted to IPRBranch.ITC337.Rulings@cbp.dhs.gov. To request information on CBP's recordation program, please contact RR at iprrquestions@cbp.dhs.gov

Guidance on CBP IPR Policy and Programs - The IPR and E-Commerce Division (IPR Division) coordinates with rights holders, members of the trade community, CBP staff, other Federal agencies, and foreign governments in developing and implementing the Agency's IPR strategy, policy and programs. To contact the IPR Division, email iprpolicyprograms@cbp.dhs.gov

e-Allegations - If you are aware of or suspect a company or individual is committing IPR crime, please report the trade violation using CBP's e-Allegations Online Trade Violation Reporting System at https://eallegations.cbp.gov/Home/Index2. Trade violations can also be reported by calling 1-800-BE-ALERT.

National Intellectual Property Rights Coordination Center - To Report Violations of Intellectual Property Rights, including counterfeiting and piracy, contact the National IPR Coordination Center at https://www.iprcenter.gov/referral/ or telephone 1-866-IPR-2060.

U.S. Customs and
Border Protection

CBP Publication No. 1542-0921

EXHIBIT 3

frontier economics

THE ECONOMIC IMPACTS OF COUNTERFEITING AND PIRACY

Report prepared for BASCAP and INTA

Acknowledgements

Frontier Economics Ltd is a member of the Frontier Economics network, which consists of two separate companies based in Europe (Frontier Economics Ltd, with offices in Brussels, Cologne, Dublin, London & Madrid) and Australia (Frontier Economics Pty Ltd, with offices in Melbourne & Sydney). Both companies are independently owned, and legal commitments entered into by one company do not impose any obligations on the other company in the network. All views expressed in this document are the views of Frontier Economics Ltd.

The International Chamber of Commerce (ICC) works to promote a balanced and sustainable system for the protection of intellectual property. It believes that IP protection encourages innovation and the development of knowledge-based industries, stimulates international trade, and creates a favorable climate for foreign direct investment and technology transfer. ICC launched BASCAP (Business Action to Stop Counterfeiting and Piracy) to connect and mobilize businesses across industries, sectors and national borders in the fight against counterfeiting and piracy. Visit BASCAP on the web at: www.iccwbo.org/bascap

The International Trademark Association (INTA) is a global organization of over 7,000 trademark owners and professionals from over 190 countries. INTA is a not-for-profit membership association dedicated to supporting trademarks and related intellectual property in order to protect consumers and to promote fair and effective commerce. The Association was founded in 1878 and today INTA leads the way in global trademark research, policy development, education and training. More details about INTA and its roles are available at www.inta.org

BASCAP and INTA express appreciation to TECXIPIO for their valuable source data contributions to this report. TECXCIPIO is an IT company specialized in building scalable solutions to accurately track and analyse worldwide copyright infringements on the internet. www.tecxipio.com

CONTENTS

Foreword

When BASCAP commissioned Frontier Economics to do a report in 2011 on the global impact of counterfeiting and piracy, our aim was firstly to build on the seminal work of the OECD to—for the first time ever—undertake a data-based, econometric approach to quantifying the value of counterfeiting and piracy; secondly, we set out to pick up where the OECD left off, by expanding their work to include several categories of counterfeiting and piracy that they did not address. Our findings were somewhat alarming, in terms of the magnitudes, but also the projections of how the problem of counterfeiting and piracy would continue to grow in the years to follow. At that time, Frontier estimated that the total global economic value of counterfeit and pirated goods was as much as $650 Billion per year, and projected that this figure would grow to almost $1.8 Trillion by 2015.

As 2015 drew to a close, BASCAP, together with the International Trademark Association (INTA), asked Frontier, to update their report. They have found that counterfeiting and piracy continue to grow at an astounding rate. And, despite increased efforts by the private sector, governments, international government organizations and a growing number of NGOs, the problem is getting worse, not better.

This troubling trend was confirmed last year when OECD/EU IPO issued a report updating their original 2008 report on the level of international trade in counterfeit goods, where they found an 80% increase in counterfeiting between 2008 and 2013.

In developing this report, Frontier has once again collaborated with OECD on methodologies and once again addressed additional impacts of counterfeiting a piracy beyond losses associated with cross border trade in fakes. Additionally, the new Frontier study takes a deeper look into the broader social economic impacts of counterfeiting and piracy.

This report shows that the infiltration of counterfeit and pirated products, or *IP theft,* creates an enormous drain on the global economy – crowding out Billions in legitimate economic activity and facilitating an "underground economy" that deprives governments of revenues for vital public services, forces higher burdens on tax payers, dislocates hundreds of thousands of legitimate jobs and exposes consumers to dangerous and ineffective products.

We commissioned the original Frontier report and this update because we believe that reliable information on the scope, scale, costs and impacts of counterfeiting and piracy is critical for helping policymakers to better understand that the trade in fakes is damaging their economies, threatening the health and safety of their citizens and stifling innovation and creativity.

BASCAP and INTA hope that better information on how counterfeiting and piracy undermine IP, innovation, economic growth and employment, will better enable policymakers to make the fight against IP theft a higher public policy priority – and take the actions needed to prevent the damage inflicted by counterfeiting and piracy.

BASCAP and INTA will continue to explore ways to add further research on this critical issue, and to work together and with other stakeholders to build greater awareness of the enormous costs of counterfeiting and piracy.

EXECUTIVE SUMMARY

Counterfeiting and piracy are highly pervasive across countries and sectors, representing a multi-Billion-dollar industry globally that continues to grow. Measuring the scale of counterfeiting and piracy helps us to understand the size of the problem, and the related social costs. It also helps inform policymakers so that they can target resources appropriately towards combating counterfeiting and piracy.

1.1 Extending the findings of the OECD/EUIPO

Our starting point is the recent work undertaken by the Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office (EUIPO) to measure the extent of piracy and counterfeiting in international trade.[1] The OECD/EUIPO Report builds on a previous, ground-breaking study by the OECD in 2008. Since the publication of the initial report, researchers at the OECD have been able to bring significant enhancements to their research methodology, including improved econometric modelling, greater magnitudes of data and increased primary data from customs experts.

The OECD/EUIPO estimates that trade in counterfeit and pirated products accounted for as much as 2.5% of the value of international trade, or $461 Billion, in 2013.[2] Notably, this figure represents an increase of more than 80% over the OECD's findings in 2008.

Our report seeks to quantify the global value of counterfeiting and piracy and related economic and social costs. As revealing as the OECD/EUIPO Report is, its focus is on one specific aspect of counterfeiting and piracy: the international trade of counterfeits across borders.

We therefore draw on and extend the OECD/EUIPO Report to include additional types and impacts of counterfeiting and piracy delineated, but not quantified, in their analysis. Specifically, this study quantifies three additional categories of losses: (i) the value of domestically produced and consumed counterfeit goods, (ii) the value of digital piracy, and (iii) wider economic impacts. Our approach and analysis is a follow-on study from our 2011 report for BASCAP, which built on the OECD's 2008 analysis.

Our analysis consists of the following four dimensions.

- **Quadrant 1: Internationally traded counterfeit and pirated goods.** We reprise the OECD/EUIPO's recent estimates of the value of counterfeit and pirated physical goods in international trade. This captures the value of counterfeit goods that cross international borders. We also develop projections of this value to 2022.
- **Quadrant 2: Domestically produced and consumed counterfeit and pirated goods.** We estimate the value of domestically produced and consumed counterfeit and pirated goods using the findings of the OECD/EUIPO Report as a starting point. This

[1] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. Available at: http://dx.doi.org/10.1787/9789264252653-en. (hereinafter "OECD/EUIPO Report")

[2] Ibid.

captures the value of counterfeits that are produced and consumed within the borders of a country.

- **Quadrant 3: Piracy distributed through the Internet, mainly by peer-to-peer (P2P) sharing and streaming.** We estimate the value of digital piracy in film, music, and software, which is not captured in the OECD/EUIPO Report as it is based on physically traded goods. Our analysis draws on industry data and studies.
- **Quadrant 4: Wider economic and social impacts.** Building on the magnitudes calculated in quadrants 1-3, we measure related economic and social impacts of counterfeiting and piracy. Specifically, we:
  - Develop an econometric estimate of the impact of counterfeiting and piracy on foregone economic growth.
  - Present effects of the displacement by counterfeiting and pirating activities of legitimate activities on employment, FDI, and sales tax revenues.
  - Estimate costs of criminality related to counterfeiting and pirating activities

1.2 Key findings

Our analysis shows that the scale of counterfeiting and piracy globally is large, that it has grown since previous estimates, and that this growth is expected to continue. Our estimates of these values across all four quadrants are shown in Table 1.S below.

We estimate that the value of international and domestic trade in counterfeit and pirated goods in 2013 was $710 -$ 917 Billion. We estimate that, in addition to this, the global value of digital piracy in movies, music and software in 2015[3] was $213 Billion.

We estimated wider economic costs associated with the effects of counterfeiting and piracy on the displacement of legitimate economic activity. This estimate also provides a starting point for inferring fiscal losses. We also estimated the effects of counterfeiting and piracy on Foreign Direct Investment (FDI) and crime. The results are reported in Table 1 below.

[3] Digital piracy is calculated from 2015 data, which is the most recently available data

Table 1.Summary of estimates of counterfeiting and piracy

Quadrant	Estimate	2013	2022 (forecast)
1	Total international trade in counterfeit and pirated goods	$461 Billion	$991 Billion
2	Total domestic production and consumption of counterfeit pirated goods	$249 - $456Billion	$524 - $959 Billion
3	Digital piracy in movies, music and software	$213Billion	$384 - $856 Billion
	- Digital piracy in film	$160 Billion	$289-644 Billion
	- Digital piracy in music	$29 Billion	$53-117 Billion
	- Digital piracy in software	$24 Billion	$42-95 Billion
	Total value of counterfeit and pirated goods	**$923 Billion – 1.13 Trillion**	**$1.90 -$2.81 Trillion**
4	Wider economic and social costs		
	- Displacement of legitimate economic activity	$470-$597 Billion	$980-$1244 Billion
	- Estimated reduction in FDI	$111 Billion	$231 Billion
	- Estimated fiscal losses	$96-$130 Billion	$199-$270 Billion
	- Estimated costs of crime	$60 Billion	$125 Billion
4	**Total Wider economic and social costs**	**$737-$898 Billion**	**$1.54 - $1.87 Trillion**
	Estimated employment losses	**2-2.6 million**	**4.2-5.4 million**
	Foregone economic growth in OECD 2017	**$30 Billion to $54 Billion**	

Source: Frontier estimates based on OECD 2013 data on counterfeiting in international trade, and UN trade and GDP data to derive estimates for domestic production and consumption. Data for Piracy based on latest industry sources (2015).

We find significant effects on the job market through the displacement of legitimate economic activity by counterfeiting and piracy. We estimate net job losses in 2013 to lie, globally, between 2 and 2.6 million, and we project net job losses of 4.2 to 5.4 million by 2022.

We also estimated the effects of changes in the incidence of counterfeiting and piracy on economic growth. Our econometric model, estimating the impact of changes in the intensity of counterfeiting and piracy on economic growth, suggests that a percentage point reduction in the intensity of counterfeiting and piracy would be worth between $30 Billion to $54 Billion in 2017 for the 35 OECD countries.

Table 1 also reports forward projections out to the year 2022.

Our forward projections begin with OECD/EUIPO's estimates of international trade in counterfeit and pirated goods, augmented by forecasts of growth in import volumes and the ratio of customs seizures to real imports. Using these, we forecast that the value of trade in counterfeit and pirated goods could reach **$991 Billion** by 2022.

We carry out a similar exercise to illustrate how the size of domestic production and consumption of counterfeit and pirated goods may change over time. We use data on recent and forecast rates of growth in global trade and GDP, and projected growth in the rate of counterfeiting. Using this approach, we forecast that the value of domestically produced and consumed counterfeit and pirated goods could range from **$524 - $959 Billion** by 2022.

Applying the methodology used in our previous study, we combine two different approaches to project digital piracy into the future. The first approach assumes that digital piracy will maintain its share of total counterfeiting and piracy over time. The second approach assumes that digital piracy grows proportionally to global IP traffic. Combining these two approaches, we forecast that the value of digital piracy in movies, music and software could reach from **$384 - $856 Billion** by 2022.

1.3 Analytical approach

As recognised in the OECD/EUIPO Report, the estimation task is necessarily complicated by the fraudulent nature of counterfeiting, which relies on the activity being hidden from view. The OECD/EUIPO Report addresses this challenge via an innovative analytical approach that uses data on customs seizures. Individual sectors have also relied on surveys to understand the scale of counterfeiting and piracy that they face, as well as collecting data on the prevalence of counterfeiting and piracy as part of their routine IP enforcement activities.

To estimate the scale and impacts of counterfeiting and piracy, we use and build on the OECD/EUIPO Report, bringing in additional publicly available data from reputable sources such as the UN Statistics Division. We have drawn on industry data to develop our estimates of digital piracy. Throughout our analysis, we have engaged closely with relevant sector bodies to ensure that our approach is robust and the data sources are reliable.

To account for the significant uncertainty around the value of counterfeiting and piracy, we use conservative assumptions in our estimates, and provide ranges for our estimates. The main report sets out the data sources and assumptions used in detail, and the impact of the assumptions made on the interpretation of our analysis.

1.4 Agenda for future research

It is important to continue to highlight the scale of the challenge posed by counterfeiting and piracy globally. We believe that a number of next steps are important, including the following.

- Further research into the prevalence of counterfeiting and piracy of physically traded goods that don't cross borders. Our analysis infers the prevalence of

domestically produced and consumed counterfeits using the OECD/EUIPO analysis of internationally traded counterfeits. Further research would help ensure more precise estimates of the scale of domestic counterfeiting in future.

- The digital piracy landscape is changing rapidly. Further data collection and analysis to understand the scale of growing forms of digital piracy (e.g. gaming, copyright infringing user generated content, TV series) would help policymakers to better address policies to the problem of digital piracy.
- Further analysis of and improvements to the customs seizures data that underlies the OECD/EUIPO analysis would be beneficial, for example in helping policymakers build up a picture of how prevalence of counterfeiting in different sectors and geographies varies year on year.

2 INTRODUCTION

2.1 Background and context

Counterfeiting and piracy are a form of theft. They involve the illegitimate acquisition and use of intellectual property (IP). The economic and social costs of counterfeiting and piracy are thus similar to those associated with other types of theft (e.g. personal property theft). Counterfeiting and piracy divert private and public resources which could otherwise be used for more productive ends, into the illegal acquisition of IP, or defending IP from such illegal acquisition.[4]

However, the economic costs of counterfeiting and piracy extend well beyond these traditional costs of theft. First, they reduce the returns to innovation. While there are ongoing debates about the optimal level of IP protection to balance the rights of innovators and the users of IP, counterfeiting and piracy hurts *both* the innovator and the user. The economic costs of IP erosion through counterfeiting and piracy are particularly severe in knowledge-driven economies.

Secondly, whereas classical analyses of property theft treat the theft itself as a transfer – and therefore not in and of itself a cost – in practice, that approach is not valid in the case of counterfeiting and piracy. This is because of the close links between counterfeiting activities and other forms of criminal activities. Thus, counterfeiting and piracy are a "cost" not a transfer because they stimulate other "costs", i.e. activities that adversely impact on social well-being.

Counterfeiting and piracy are therefore specific economic and social "bads". Measuring the size of counterfeiting and piracy is therefore important for several reasons.

- First, it helps us to understand the size of the problem. The extent of these activities is an indicator of the extent to which IP is eroded globally, and a measure of the extent to which productive resources and consumption are diverted to illicit activities.
- Secondly, measuring the magnitude of the problem serves as a platform for measuring related costs. These include the social costs associated with the displacement of employment in legal activities, the economic costs of the erosion of IP, and the social costs associated with criminal activities linked to counterfeiting and piracy.

Thus, measuring the extent of this problem helps us to draw inferences as to the extent of the economic and social costs arising from counterfeiting and piracy. This helps inform policymakers so that they can target resources appropriately towards combating counterfeiting and piracy.

In order to do this, this report begins by building on the recent, ground-breaking work undertaken by the OECD and EUIPO to measure the extent of piracy and counterfeiting

[4] See in particular Gordon Tullock (1967), "The welfare costs of tariffs, monopolies, and theft", Western Economic Journal, Vol 5.3

in international trade.[5] As revealing as the OECD/EUIPO Report is, it only focuses on one specific aspect of counterfeiting and piracy, namely that related to the *international* trade of these products across borders. This report extends the analysis to consider other dimensions, as described below.

2.2 Extending the findings of the OECD/EUIPO: estimating the global incidence of counterfeiting and piracy and its effects

We draw on and extend the OECD/EUIPO Report to estimate the following dimensions of counterfeiting and piracy globally.

- **Quadrant 1: Internationally traded counterfeit and pirated goods.** We report the OECD/EUIPO's estimates of the value of counterfeit and pirated physical goods in international trade. This captures the value of counterfeit goods that cross international borders. We also develop projections of this value to 2022.
- **Quadrant 2: Domestically produced and consumed counterfeit and pirated goods.** It is necessary to compute this value as it provides an indication of the true size of the counterfeit economy by capturing the level of counterfeits that are produced and consumed within the borders of a country. This is especially true of larger economies, in which trade is a lower proportion of GDP than is the case in smaller economies. In section 3.2 we develop a methodology for inferring the value of domestically produced and consumed pirated goods using the findings of the OECD/EUIPO Report as a starting point. This captures the value of counterfeits that are produced and consumed within the borders of a country.
- **Quadrant 3: Piracy distributed through the Internet, mainly by peer-to-peer (P2P) sharing and streaming.** It is necessary to focus on this specifically because the OECD/EUIPO Report analysis is based on physically traded goods, i.e. ones that are transported from point to point. However, for sectors such as film, music, and software, physical transportation is not the only or even primary mode of disseminating products. We therefore need to consider the role illegal online activity plays in substituting for legitimate modes of distribution and consumption – whether physical or online – to estimate the true size of piracy. Section 4 sets out our analysis of digital piracy, which focuses on digital piracy in film, music, and software.
- **Quadrant 4: Wider economic and social impacts.** Building on the magnitudes calculated in quadrants 1-3, we measure related economic and social impacts of counterfeiting and piracy. These include costs related to displacement of employment, erosion of intellectual property (IP), and criminal activities linked to counterfeiting and piracy. This is done in section 5.

In the remainder of the report, we describe our analysis of each quadrant in turn. In the concluding section, we project our estimates forward to 2022 to provide an indication of

[5] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris. Available at: http://dx.doi.org/10.1787/9789264252653-en. (hereinafter "OECD/EUIPO Report")

how counterfeiting and piracy is likely to develop over time; results are summarised across all four quadrants.

3 QUADRANTS 1 AND 2: THE GLOBAL VALUE OF COUNTERFEITING AND PIRACY

3.1 Quadrant 1: The OECD/EUIPO's estimates of international trade in counterfeit and pirated goods

The first category of estimates, as referenced in section 2.1, are derived directly from the research undertaken by the OECD and the EUIPO, on the extent of counterfeiting in international trade.[6] The OECD/EUIPO Report estimates that trade in counterfeit and pirated products accounted for as much as 2.5% of the value of international trade, or $461 Billion, in 2013.[7] In the report, China emerged as the primary origin of counterfeits imported into the EU. This is in line with US customs seizures data, which shows that 52% of seized counterfeit imports into the US originated from China.[8]

$461bn

The OECD/EUIPO estimates that international **trade in counterfeit and pirated products** accounted for as much as 2.5% of the value of international trade, or $461 Billion, in 2013.

The range of products found to be affected by counterfeiting and piracy is broad. Affected goods span luxury consumer products such as leather goods, common consumer products such as toys and pharmaceuticals, and business-to-business products including spare parts and chemicals.

Similarly, the OECD/EUIPO Report found that counterfeit and pirated products originate from nearly all economies. However, there is variation in prevalence by geography. It found higher prevalence of counterfeiting in trade in the EU, estimating that counterfeit and pirated goods accounted for up to 5% of imports in the EU, or $116 Billion, in 2013. Middle-income and emerging economies were often found to be transit points or producing economies of internationally traded counterfeit and pirated goods.

Comparison of the 2013 estimates with previous analysis by the OECD indicates increasing counterfeiting and piracy in international trade over time. The OECD estimated that in 2008, internationally traded counterfeit and pirated products represented up to 1.9% of global imports, or $200 Billion.[9] The 18% annual estimated

[6] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris.

[7] Ibid.

[8] For the fiscal year 2015, measured by value (the manufacturer's suggested retail price). US Department of Homeland Security, Intellectual Property Rights Seizure Statistics, Fiscal Year 2015.

[9] OECD (2008), The Economic Impact of Counterfeiting and Piracy.

growth is likely driven in part by the ongoing priority assigned to IP crimes and the lack of additional resources committed to IPR enforcement since the 2008 report. Other factors include revival in trade following the 2008 crisis, and growth in e-commerce. We project the OECD/EUIPO estimates forward in Section 6.1 to provide an indication of likely future growth in traded counterfeits. We forecast that the value of trade in counterfeit and pirated goods could reach $991 Billion by 2022.

3.1.1 Comments on methodology

The OECD's analysis of 2008 was ground-breaking: it was the first attempt to systematically estimate the incidence of counterfeiting and piracy in international trade. The estimation task is necessarily complicated by the fraudulent nature of the trade in fakes, which relies on the activity being hidden from view. Since the publication of the initial report, researchers at the OECD have been able to bring significant enhancements to their research methodology, including improved econometric modelling, greater magnitudes of data and increased primary data from customs experts.

The latest estimates published in the OECD/EUIPO Report benefit from improved data relative to the 2008 study, which meant that the assumptions required to estimate trade in counterfeit and pirated products were less restrictive. One of the implications is that the 2008 and 2013 estimates are not fully comparable, as some changes in the estimates could be attributable to these data and methodology improvements.

The OECD/EUIPO Report used three main sources of evidence:

- customs seizures data from:
  - the World Customs Organization (WCO),
  - the European Commission's Directorate-General for Taxation and Customs Union (DG TAXUD), and
  - the United States Department of Homeland Security (DHS);
- world trade data from the United Nations (UN) Comtrade database; and
- qualitative evidence from structured interviews with customs officials.

We outline the key changes in assumptions between the estimates of counterfeiting and piracy in 2008 and 2013 in Table 15 below. It shows that the recent OECD/EUIPO Report benefits from separate estimates of traded counterfeit and pirated products for 2011, 2012 and 2013, as well as improved availability of evidence to use in estimating relative and actual counterfeiting and piracy propensities. The previous strong assumption of minimum counterfeiting rates where data was missing resulted in an overestimate of overall counterfeiting. By relaxing this strong assumption, the OECD/EUIPO's more recent analysis is more accurate, although the change in assumptions also limits the comparability of the new and old estimates over time.

Some important assumptions remain, in particular the use of a 'fixed point' to estimate actual counterfeiting propensities. See box in Section 3.2.1 for a description of the approach to estimating the fixed point.

Table 2. Improvements in the approach between 2008 and 2016

Aspect of analysis	Assumptions and approach in 2008	Assumptions and approach in 2016
Time dimension	Data was pooled to produce an estimate for 2008 only.	Data not pooled, separate estimates are available for 2011, 2012 and 2013.
Estimation of *relative* counterfeiting propensity	Relative propensities were estimated using data on the value of seized goods, numbers of seizures and numbers of seized goods. This required assumptions to convert quantity data to monetary values. Non-zero minimum levels of counterfeiting were assumed where data was missing. This strong assumption resulted in potential overestimates of counterfeiting.	Relative propensities were estimated using data on the value of seized goods. This avoided the need for assumptions to convert quantity data to monetary values. More reasonable assumption on minimal levels of counterfeiting was used, due to improved data quality. This results in more accurate estimates of counterfeiting.
Estimation of *actual* counterfeiting propensity	Relative propensities were converted to actual propensities using a single estimate of the actual rate of counterfeits in exports of one good from one economy (the 'fixed point') to one of its export partners. The fixed point was selected based on informal interviews.	The approach remains the same, but the fixed point was selected based on structured interviews and focus groups with customs and enforcement officials.

Source: Adapted from Table 3.2, OECD/EUIPO Report

Note: The 'fixed point' is the estimated actual counterfeiting propensity for the economy/product pair with the highest expected rate of counterfeiting. See Section 3.2.1 for full explanation.

3.2 Quadrant 2: estimating the domestic production and consumption of counterfeit and pirated goods

We extend the OECD/EUIPO analysis to estimate the value of counterfeit and pirated goods that are both produced and consumed domestically, i.e. goods that are *not* traded across international borders. While the OECD/EUIPO did not include analysis of domestically produced and consumed counterfeiting and piracy, they acknowledge that more investigation was needed into this area. Alternative models and existing data can be used to estimate the value of domestic counterfeiting and piracy. Calculating this value provides an additional indication of the true, global size of the counterfeit and piracy economy.

In this section, we describe:

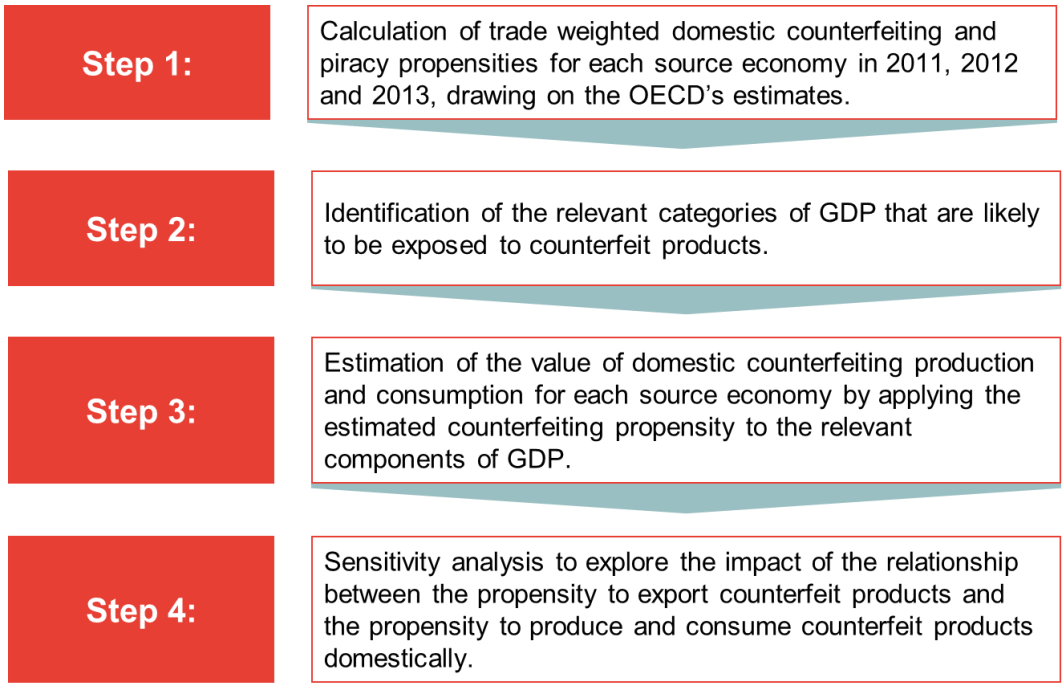
- the approach we have taken to estimating the scale of domestic production and consumption of counterfeit goods;
- the data sources our estimates draw on; and
- the results of our analysis.

3.2.1 Methodology

Limited or non-existent government or other conventional sources of data presents a challenge to estimating magnitudes of counterfeiting and piracy in this quadrant. Consequently, to address the significant uncertainties associated with estimating the scale of domestic counterfeiting and piracy, we bring together the best available data sources, presenting estimates as ranges where appropriate.

We once again start with and build on the OECD/EUIPO's estimates of internationally traded counterfeiting and piracy. This follows the approach used in our previous analysis.[10] The analysis follows four steps, shown in Figure 1 below. As explained in section 3.2.2 below, we supplement OECD data with data from the United Nations on GDP and Comtrade, to arrive at an estimate for domestic counterfeiting.

Figure 1: Approach to estimating domestic counterfeiting and piracy



Source: Frontier Economics

To estimate domestic counterfeiting propensities, we start from the OECD/EUIPO's estimates of the maximum relative propensity of economies to export counterfeit and pirated products. This information is summarised in two indices developed by the OECD:

[10] Frontier Economics for BASCAP, 2011, Estimating the global economic and social impacts of counterfeiting and piracy

- the GTRIC-p index, which shows the relative propensity of world trade to be counterfeit for different products; and
- the GTRIC-e index which shows the relative propensity of internationally traded counterfeit products to originate from different source economies.

The indices can be combined to estimate relative counterfeiting propensities for each source economy and product combination. For example, the GTRIC-p index shows that, in 2013, counterfeit footwear was 1.9 times more likely to originate from China than India.

To estimate absolute counterfeiting propensities, the OECD/EUIPO use a "fixed point." We describe the fixed point and the approach to estimating it in the box below.

ESTIMATING THE "FIXED POINT"

The GTRIC estimates show *relative* counterfeiting propensities. To convert these into estimates of *absolute* counterfeiting propensities, the OECD/EUIPO use a "fixed point." This is the actual counterfeiting rate for the source economy and product combination with the highest rate of counterfeiting.

The highest rate of counterfeiting was estimated to be for exports of footwear from China. It was found that, for some EU members, the rate of counterfeits in total imports of footwear from China reached 27%.

The OECD/EUIPO assume that this counterfeiting rate applies to all other shoes exported from China, i.e. to non-EU members importing shoes from China. The "fixed point" therefore represents an upper bound estimate of absolute counterfeiting.

All other *actual* counterfeiting rates are estimated using their relative counterfeiting propensity compared to the relative and actual counterfeiting rate for exports of shoes from China. For example, the actual rate of counterfeiting for clothes from China is estimated as:

> *(Relative counterfeiting propensity for clothes from China / Relative counterfeiting propensity for shoes from China) * Actual counterfeiting propensity for shoes from China*

This methodology is repeated to provide estimates of actual counterfeiting rates for all economies and products. Given that the fixed point represents the maximum counterfeiting rate, our analysis of the value of domestic counterfeiting production and consumption using this approach should be interpreted as providing an upper estimate.

3.2.2 Data sources

We use a number of data sources to estimate the value of domestic counterfeiting and piracy, which we describe below.

OECD/EUIPO estimates of counterfeiting and piracy propensities

The OECD/EUIPO Report provides the GTRIC-e and GTRIC-p indices of relative counterfeiting propensities in world trade which underpin its estimates.[11] We combine these indices to form the GTRIC matrix which sets out the relative counterfeiting propensity for each economy and product pair. We then use the estimated "fixed point" to convert the relative counterfeiting propensities into absolute counterfeiting propensities for each source economy and product pair.

UN GDP data

We use UN GDP data from the UN Statistics Division Statistical Database.[12] For each economy, this reports gross value added, broken down by the International Standard Industrial Classification of All Economic Activities (ISIC).

The product classification used in the OECD/EUIPO Report is based on identifying products sensitive to counterfeit trade at the HS classification level.[13] HS product classifications are relevant to world trade, but they do not map directly to ISIC GDP classifications. In line with our previous analysis, we therefore focus on one category of GDP – manufacturing (ISIC D).

This approach captures the most relevant and sensitive product categories identified by the OECD/EUIPO Report, although it also includes some products that are not found to be sensitive. This means that our estimates of the value of domestic counterfeiting and piracy should be interpreted as upper estimates.

Comtrade data

Applying estimated counterfeiting propensities to GDP data requires that the propensity estimates are available at the economy level, rather than the product level. We estimate economy level counterfeiting propensities by first estimating the value of counterfeiting and piracy for each combination of product, economy and year. We then aggregate the estimated value of counterfeit trade for each economy and year, and divide this by the value of all trade for the corresponding economy and year. To do this, we draw on UN Comtrade data on the value of global imports by source economy, year and HS code.[14]

Where economies are excluded from the OECD/EUIPO Report analysis or Comtrade data is not available for them, they are not included in our domestic estimates. To estimate the value of domestic counterfeiting and piracy globally, we therefore scale up our estimates to account for the ISIC D GDP represented by these economies. We find that 1-2% of ISIC D GDP is excluded in each year before making this adjustment. In doing this, we are assuming that countries are excluded due to data limitations and that their counterfeiting rates are in line with international averages.

---

[11] OECD/EUIPO (2016), Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD Publishing, Paris.

[12] UN Statistics Division Statistical Databases - National Accounts Main Aggregates - Value added by Economic Activity

[13] The Harmonized Commodity Description and Coding Systems (HS) is an international nomenclature for the classification of traded goods on a common basis for customs purposes.

[14] United Nations Statistics Division, Comtrade data in US dollars.

Industry studies and engagement

Our analysis assumes that there is a direct mapping from the propensity of an economy to export counterfeit and pirated products to its propensity to produce and consume counterfeit products domestically. For some goods or economies, this assumption may not hold – for example in larger economies for which international trade is a smaller share of GDP.

We have therefore drawn on industry studies and engagement to explore the impacts of varying this assumption.

3.2.3 Results

Using the approach described above, we estimate that the total scale of domestic production and consumption of counterfeit and pirated products in 2013 was **$249 - $456 Billion**. This range reflects uncertainty over the relationship between traded and domestically produced counterfeit and pirated products.

$249-456bn

We estimate that the total scale of **domestic production and consumption** of counterfeit and pirated products in 2013 was $249 - $456Billion.

Our previous analysis estimated that the value of domestic counterfeiting and piracy in 2008 was between $140 and $215 Billion.[15] This suggests growth in domestic counterfeiting over time, although our previous estimates are not fully comparable with the updated estimate due to changes in the data and methodology used by the OECD/EUIPO.

Comparing estimates between 2011 and 2013 also indicates growth in domestic counterfeiting over time, with our analysis suggesting that the value of domestic counterfeiting and piracy in 2011 was $193 - $354 Billion. Again, this comparison should be treated with caution, as changes between 2011 and 2013 could be partly driven by changes in the quality of customs enforcement and data collection year on year.

Our upper bound estimate of domestic counterfeiting and piracy, of **$456 Billion**, is underpinned by the assumption that counterfeiting propensities are the same for goods that aren't traded across international borders as for those that are internationally traded.

In practice, this may not always hold, as the structure of traded and domestic counterfeiting production may not be the same in every economy. We engaged with industry stakeholders across a range of sectors to explore how far this assumption may be valid. We found that the structure of counterfeiting production can vary substantially by product type. For example, food and beverage products are typically developed to suit local tastes, resulting in domestically focused production. In turn, this can result in

[15] Not adjusted for inflation.

production of counterfeits being predominantly for domestic rather than international markets. In contrast, for generic consumer electronics, counterfeit production may focus both on domestic and international markets, with the latter potentially combined with assembly taking place in a local market. This can make it difficult to identify whether counterfeit production takes place in a domestic or external market.

Data allowing comparison of counterfeit prevalence between goods produced and consumed domestically versus internationally traded goods is limited. However, some stakeholders noted that they had observed particularly high rates of domestic counterfeiting for specific product categories, higher than the OECD/EUIPO prevalence rates developed for internationally traded goods. While there wasn't sufficient data available for us to test this in our analysis, it implies that our approach of assuming that domestic and international counterfeiting rates are equal may be conservative. More data would be required for specific product categories to confirm this.

To provide a contrasting sensitivity test of our results, in line with our previous analysis, we draw on a study by the Japan Patent Office (JPO). We apply two key findings to our analysis, as follows.[16]

- The JPO study found that counterfeiting and piracy is more prevalent in traded products than domestically consumed and produced products. It found that firms encountered domestically produced counterfeit products at 54.6% of the rate at which they encountered imported counterfeit products. Applying this proportion to all economies in our analysis generates our lower estimate of the global value of domestic counterfeiting and piracy in 2013, of **$249 Billion**.
- The study found that this relationship between traded and domestic counterfeiting varied by geography, so that in practice some economies see higher prevalence of domestic than traded counterfeits and others see the opposite. It found that in Asia domestically produced counterfeit products are more likely to be exported than consumed domestically, while the opposite is true outside Asia. As an alternative sensitivity test to the one described above, we apply these parameters (shown in Table 3 below) to our analysis. This scales down our estimates of domestic counterfeiting in Asia, and scales up our estimates of domestic counterfeiting in the rest of the world up, resulting in an estimate of the value of domestic counterfeiting and piracy in 2013 of **$310 Billion**. Even with this assumption, China still accounts for the largest share of the global total, at $143 Billion, or 46%.

Table 3. Breakdown of domestic counterfeit production into domestic consumption and exports

Region	% of counterfeit goods produced that are:	
	Consumed domestically	Exported
Asia	34%	66%
Rest of world	55%	45%

Source: Frontier analysis of JPO (2005)

[16] Japan Patent Office, March 2005, FY2004 Survey Report on Losses Caused By Counterfeiting

3.3 Conclusion and discussion

Our analysis suggests that the scale of domestically produced and consumed counterfeit and pirated products is significant, substantially adding to the OECD/EUIPO's estimate of the global value of traded counterfeits. Our findings also indicate that both international trade and domestic production and consumption of counterfeit products is likely to have grown substantially since 2008, although the validity of direct comparison of our new results with our previous estimates is limited by changes in the assumptions behind the OECD/EUIPO's analysis.

Table 4 summarises the Quadrant 1 and 2 estimates of counterfeiting and piracy, and also our projections of these values in 2022. We describe our approach to developing the projections in more detail in Section 6.1.

Table 4 Summary of estimates of total traded and domestic counterfeiting

Result	2013	2022 (forecast)
Estimate of total international trade in counterfeit and pirated goods	$461 Billion	$991 Billion
Estimate of total domestic production and consumption of counterfeit and pirated goods	$249 - $456Billion	$524 - $959 Billion

Source: Frontier estimates based on OECD 2013 data on counterfeiting in international trade, and UN trade and GDP data to derive estimates for domestic production and consumption.

4 QUADRANT 3: THE GLOBAL VALUE OF DIGITALLY PIRATED GOODS IN SPECIFIC SECTORS

4.1 Introduction

The OECD/EUIPO Report did not cover digital piracy, and called for separate analysis into its magnitude. In this section we estimate the economic "size" of digital piracy in the following sectors: film, music, and software. By "size" we mean the dollar value of pirated sales in these sectors, which is not the equivalent of economic losses to the legitimate industries.

Since pirated sales do not occur through traditional markets, the value of these sales needs to be inferred. An estimate of the volume of transactions and of their price is therefore required. Estimates of these will need to draw on data sources that are specific to each type of activity. These estimates tell us how big the piracy problem is in terms of the overall market for pirated goods. They do not, however, in and of themselves tell us how big the damage is to holders of IP. What they do provide is an estimate, even if partial, of the magnitude of these "underground" activities, and an indication of the potential value that could be appropriated by rights holders if piracy were to be eliminated. As explained in section 5.1, these estimates also provide a starting point for estimating the costs of piracy to society as a whole.

The three sectors which we focus on — film, music, and software — are sectors where digital piracy has a particularly significant impact, and these sectors account for the bulk of digital piracy. They are also ones for which it is possible to develop reasonable piracy estimates derived from data reported by various market sector participants and data aggregators. We signpost other (currently emerging) areas of piracy throughout the chapter, but a detailed analysis would exceed the scope of this study. We have used the most recent and robust data available from industry sources, which is from the year 2015.

4.2 Film

In the following, we first provide an overview of recent research findings on the impact of piracy in film. We then estimate the commercial value of piracy in film using a "bottom up" approach.

$160bn

We estimate that the commercial value of **digital piracy in film** in 2015 was $160 Billion.

4.2.1 Background to piracy in film

"The general industry evidence appears consistent with a hypothesis that piracy has hurt the movie industry." This statement, taken from Liebowitz (2013)[17], is based on the fact that the introduction of BitTorrent in 2003-04 has coincided with a turning point in the development of film industry revenues. Revenues for sales and rentals of pre-recorded movies in the U.S. declined by more than 20%[18] between 2005 and 2010 after having increased steadily until then. Box office revenues have remained relatively constant during the same period although a gradual 47% rise over the decade leading up to 2002 might have suggested an upward trend would have continued. It seems straightforward to attribute BitTorrent as responsible for these negative developments. However, it is likely that other developments in the market including the emergence of streaming platforms such as Netflix have also played a role in the decline of other modes of movie consumption.[19]

BitTorrent

BitTorrent is a peer-to-peer (P2P) file sharing network. It facilitates the efficient distribution of large files (e.g. entire movies or software) by breaking the files down into smaller segments and enabling users to download these "pieces" from each other rather than from a central server. Because of these characteristics, it has emerged as one of the most popular modes of digital piracy.

As a result, as Liebowitz and several other researchers have noticed, establishing the nature and size of the link between piracy and the movie industry is not as straightforward as the above trends might suggest. Academics disagree on the size of the substitution rate between pirated and purchased movies (i.e. how many fewer authorised versions a pirate would buy as a consequence of watching an unauthorised version).

Nonetheless, most researchers find movie piracy displaces legal movie sales and hence harms the movie industry. This is shown by a number of recent metastudies which are summarised in the box below.

[17] Liebowitz (2013) "The impact of internet piracy on sales and revenues of copyright owners", an abridged version of "Internet piracy: the estimated impact on sales" in *Handbook on the Digital Creative Economy* Edited by Ruth Towse and Christian Handke, Edward Elgar, 2013, p. 35

[18] Compare Liebowitz (2013), figure 2, p. 35

[19] According to Bai J. and J. Waldfogel (2009) "Movie Piracy and Sales Displacement in Two Samples of Chinese Consumers", Working Paper, The Wharton School, University of Pennsylvania, Philadelphia, PA, 'each instance of [piracy] displaces 0.14 paid consumption instances'. According to Rob R. and J. Waldfogel. (2007) "Piracy on the Silver Screen", *Journal of Industrial Economics,* Vol. 55, Issue 3, pp. 379-393, however, 'unpaid first [piracy] consumption reduces paid consumption by about 1 unit'.

METASTUDIES CONFIRM THAT PIRACY HARMS THE MOVIE INDUSTRY

- Smith and Telang (2012)[20] and Danaher, Smith and Telang (2013)[21] conclude that almost all papers that they assess find media piracy to harm sales.
- In 2015[22] the same authors find that out of 21 papers that have examined the link between piracy and sales and were accepted into peer-reviewed journals up to 2014, eighteen find a negative impact and only three find none.
- Liebowitz (2013) arrives at a similar result: Out of the seven articles identified on the impact of piracy on box office revenues or video sales/rentals, all find piracy to be harmful. His analysis leads him to conclude that the harm from piracy to the movie industry is large.

Perhaps the best empirical proof of a negative relationship between piracy and legal sales was the shutdown of Megaupload, a major cyberlocker and filesharing site, in 2012.[23] Danaher and Smith's (2013)[24] analysis attributes increases of between 6.5 to 8.5% in revenues of three large film studios in the first 18 weeks following the closure of Megaupload. This shows that some consumers turn to legal methods of movie acquisition when a major filesharing site has shut down and by extension that online movie piracy displaces digital movie sales.

The following example gives an idea of the scale of harm that can be caused by movie piracy.

ECONOMIC CONSEQUENCES OF MOVIE PIRACY IN AUSTRALIA

In 2011 a study[25] estimated the impact of movie piracy on the Australian economy, based on a survey with 3,500 adults. It found that:

1. some people pirate movies but watch authorised versions afterwards; and
2. only 45% of pirates claim they would have paid to watch authorised versions had they not been able to access a pirate version.

The study concluded that the Australian movie industry had suffered at least A$575m direct consumer spending losses in the 12 months up to Q3 2010. Adding indirect or induced impacts on other industries, movie piracy was found to have caused losses to the total Australian economy of at least A$1.3 Billion in Gross Output (Sales) and 6,100 Full Time Equivalent jobs.

---

[20] Smith M. D. and R. Telang (2012) "Assessing The Academic Literature Regarding the Impact of Media Piracy on Sales"

[21] Danaher B., M. D. Smith and R. Telang (2013) "Piracy and Copyright Enforcement Mechanisms", *Innovation Policy and the Economy*, Vol. 14, pp. 25-61

[22] Danaher B., M. D. Smith and R. Telang (2015) "Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions", Advisory Committee on Enforcement, Tenth Session, Geneva, November 23 to 25, 2015, World Intellectual Property Organization

[23] This event constitutes a "natural experiment" and is hence an ideal study of the impact of piracy on sales.

[24] Danaher B. and M.D. Smith (2013) "Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales"

[25] Ipsos MediaCT and Oxford Economics (2011) "Economic consequences of movie piracy in Australia", report on behalf of AFACT. The study covers not only digital piracy but also the acquisition of counterfeit/copied DVDs

In summary, there seems to be consensus on the fact that online piracy damages the movie industry.

Two related questions arising from this insight are *How big is the damage?*, i.e. how big are the business losses and wider economic effects caused by movie piracy?, and *How big is movie piracy?,* i.e. what is the value of pirated movies?. All studies cited above focus on the first question (the damage caused by piracy), while our analysis focuses on the second question.

A recent study by NetNames[26], which has been appraised positively by industry experts, has set the same focus. The study finds that in 2012, infringing bandwidth use in North America, Europe, and Asia-Pacific made up 23.8% of the total bandwidth consumed. The enormous scope of piracy is illustrated by the fact that in January 2013 alone, 432 million unique Internet users sought infringing material.

Our analysis in the following section goes beyond the NetNames findings. We determine the size of piracy not in terms of bandwidth or users but in terms of the monetary value of pirated items.

4.2.2 Estimating piracy in film

Estimating the size of piracy in film is challenging for a number of reasons. One of these is the speed at which both the licit and the illicit sides of the market have been changing since the advent of the Internet. The development of sharing and storing technologies, for example, has substantially influenced the way in which people steal IP. And the emergence of streaming platforms such as Netflix has transformed people's behaviour related to accessing and watching movies. Substitution rates and behavioural patterns in one year may no longer correctly reflect consumers' behaviour a few years later. Therefore, using the most recent data available is crucial.

To estimate the value of movie piracy, we use a "bottom-up" approach that starts from a measure of the volume of film piracy. One such measure is the number of illegal movie downloads via P2P networks, which is collected through specialist data aggregators. This volume measure is then matched with data on film prices – specifically prices associated with the activities for which pirated films are substitutes. The approach is outlined in more detail below.

An alternative methodology for calculating estimates of film piracy is a "top-down" approach which is based on the value of losses incurred through displaced sales. We can infer the commercial value of pirated films from estimated losses using assumptions on the propensity of consumers to substitute illegitimate versions of a film for legitimate versions.[27] This was the approach followed in our previous study for BASCAP. However, as estimates of conversion rates or business losses related to movie piracy have rarely been updated in recent years, such an approach would now be less reliable. We therefore favour the "bottom up" approach.

---

[26] Price, D. (2013) "Sizing the piracy universe", NetNames

[27] This propensity indicates how many illegal downloads displace a legal sale and will be referred to as "conversion rate" or "substitution rate" in the following.

The "bottom up" approach starts by using a number of illegal movie downloads per year. TECXIPIO, a company that tracks BitTorrent transactions worldwide, has recorded 18.5 Billion illegal movie downloads via BitTorrent in 2015.

P2P is the most popular method of illicit movie acquisition and BitTorrent is by far the largest P2P network. However, there are other ways of illegally downloading movies including streaming and using Cyberlockers. The NetNames[28] study mentioned above suggests that 39% of total pirating activity is done on BitTorrent. We use this estimate to scale up TECXIPIO's BitTorrent figure, arriving at **47.8 Billion illegal movie downloads in 2015** across all forms of digital movie piracy.

The final step consists of multiplying this number by an average price of legal movie consumption. A recent discussion by Liebowitz[29] suggests that this could be difficult because it is not clear what a pirated movie is a substitute for. On the one hand, watching a pirated movie provides a similar experience to watching a DVD or downloaded/streamed movie at home, which would suggest that a pirated movie is a substitute for any form of (legal) home video. On the other hand, watching a pirated movie could be considered a close substitute for going to the cinema because both provide the possibility to watch the movie as soon as possible after its theatrical release (which home video does not provide because typically movies are available for legal purchase months after their release).

In view of this ambiguity we choose to construct a weighted average price of movies across all different kinds of legal movie consumption, using information on consumers' typical movie watching behaviour from a 2015 Nielsen report on US consumer trends.[30]

Firstly, we infer how consumers split their total movie consumption across different activities. (To give an example, they spend 26% of their "movie-watching" time streaming movies and 14% watching movies in theatres.)[31] We then construct an average price, weighting the reported prices per movie for each of these activities by the shares of consumer time accorded to them. This yields an overall average price of $3.35 per movie. Multiplying this with our above estimate of the total number of illegal downloads, we obtain a **value of pirated movies of about $160 Billion**.

While it would be preferable to use global behavioural patterns and global average prices instead of US data, the required global data is extremely difficult to gather and not publicly available. However, using US data appears to be the best alternative, based on the following considerations:

1. Total filmed entertainment revenue in the US makes up 33% of the global market.[32] This is more than any other single country and means that even if one could construct a global average, this would be significantly influenced by US

[28] Price, D. (2013) "Sizing the piracy universe", NetNames

[29] Chapter 23: "Internet piracy: the estimated impact on sales" in Towse R. and C. Handke (2013) *Handbook on the Digital Creative Economy,* Edward Elgar, Cheltenham

[30] Nielsen (2015) Home Entertainment Consumer Trends, accessible through http://www.slideshare.net/JonathanBlumKurtz/home-entertaiment-consumer-trends.

[31] The full list can be found in Table 14, Annex A.

[32] PwC (2015) „Filmed entertainment – Key insights at a glance – Nr. 1", excerpt from *Global entertainment and media outlook 2015-2019*

data. In short, the US is probably the single most representative country of global figures.

2. The US is neither the cheapest nor the most expensive country in terms of media costs, so that calculations based on US figures are more likely to be close to the true global average than calculations based on, for example, European figures. For comparison, the usage of European data would suggest an average price of $5.81 (vs. the $3.35 US based price), and a total value of digital movie piracy of $278 Billion in 2015.

4.3 Music

In the following, we first report on recent developments in the music market and research findings on the link between piracy and sales. We then estimate the value of piracy in music using again a "bottom up" approach.

$29bn

We estimate that the commercial value of **digital piracy in music** in 2015 was $29 Billion.

4.3.1 Background to piracy in music

Recent developments in the music market

Looking only at the size of revenues, one could get the idea that the global recorded music industry has not changed significantly between our last report in 2011 ($14.8 Billion) and 2015 ($15.0 Billion).[33] However, some significant changes have taken place. One is that digital revenues have overtaken physical for the first time in history. Another is the rapid expansion of streaming platforms such as Spotify, Rdio and Pandora. The Nielsen Year End Music Reports 2014 and 2015[34], for example, show that on-demand music streams have tripled between 2013 and 2015 – to 317.2 Billion. In comparison, digital permanent downloads comprised 1.0 Billion singles and 0.1 Billion albums, and total physical retail units added up to only 0.1 Billion in 2015. The proportion of total US music revenues from streaming rose from 9% in 2011 to 34% in 2015.[35]

On the one hand, streaming cannibalises music sales because the permanent availability of a vast music collection makes the purchase of individual songs or albums almost unnecessary. The 23%[36] drop in digital permanent downloads and physical units shipped in the US between 2013 and 2015, provides empirical evidence of this hypothesis. On the other hand, streaming seems to erode music piracy because it satisfies consumers'

[33] The numbers stem from IFPI Global Music Report 2016. It should be remembered, however, that there was a significant decline in music revenues in the period 1999-2011 that was most likely caused by piracy via BitTorrent and its predecessors.

[34] 2014 Nielsen Music U.S. Report and 2015 Nielsen Music U.S. Report

[35] RIAA 2015 Year-End Industry Shipment and Revenue Statistics

[36] Based on RIAA 2014 Year-End Industry Shipment and Revenue Statistics (which also presents 2013 figures) and RIAA 2015 Year-End Industry Shipment and Revenue Statistics

demand for cheap, or even free, convenient access for music.[37] The drop of illegal music downloads via P2P-filesharing from 3.2 Billion in 2013 to 2.5 Billion in 2015[38] seems to support this argument. Further evidence is provided by a recent American Assembly study reporting that 48% of the people involved in both streaming and pirating in the U.S. say that they pirate less music because of the growth of streaming services. In Germany, the number is as high as 52%.[39]

Some hope that streaming will be able to commercialize the volume of music that is currently being pirated. This results in what the International Federation of the Phonographic Industry (IFPI) calls the "value gap" and what music sector groups say needs to be fixed if the music industry is to experience sustained growth in the future.[40]

What is particularly relevant about streaming in the context of this report is that it rapidly changes the way in which people access or listen to music – with resulting difficulties for researchers to keep track of legal music consumption patterns and pirating behaviour.

Link between piracy and sales

As shown above, growth in music piracy seems to be slowing down (although the overall scale of piracy remains large). Moreover, the direction and size of the link between music piracy and legal sales are even more hotly debated than for movies. As already described in the section on movie piracy above, recent metastudies[41] show that the vast majority of the literature finds Internet piracy to harm media sales. Liebowitz (2013)[42] also confirms this finding for papers focusing specifically on music. The conclusion of his analysis[43] is notable: 'On average, the findings for music are that the entire decline in sales since 1999 is due to piracy, and these values[44] tend to be in the vicinity of 50%-70% when dollars are measured in inflation adjusted units' (p. 37).

In contrast, the Joint Research Centre of the European Commission (2013)[45] finds the impact of piracy on sales to be small and positive. Using clickstream data, they find that a 10% increase in clicks on illegal downloading websites causes a 0.2% increase in clicks on legal purchasing websites. This suggests that consumers do not consider pirated

---

37 This will be further discussed below.

38 TECXIPIO data

39 The American Assembly (2013) "Copy Culture in the US & Germany"

40 IFPI Global Music Report – State of the Industry Overview 2016

41 Smith M. D. and R. Telang (2012) "Assessing The Academic Literature Regarding the Impact of Media Piracy on Sales"; Danaher B., M. D. Smith and R. Telang (2013) "Piracy and Copyright Enforcement Mechanisms," *Innovation Policy and the Economy*, Vol. 14, pp. 25-61; and Danaher B., M. D. Smith and R. Telang (2015) "Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions", Advisory Committee on Enforcement, Tenth Session, Geneva, November 23 to 25, 2015, World Intellectual Property Organization

42 Liebowitz (2013) "The impact of internet piracy on sales and revenues of copyright owners", an abridged version of "Internet piracy: the estimated impact on sales" in *Handbook on the Digital Creative Economy* Edited by Ruth Towse and Christian Handke, Edward Elgar, 2013

43 An important part of his analysis was converting the results of all papers into a common metric: "the share of the total industry decline that was estimated to be due to filesharing", p. 36

44 "value" here again refers to the share of total industry decline attributed to filesharing

45 Aguiar L. and B. Martens (2013), "Digital Music Consumption on the Internet: Evidence from Clickstream Data", JRC Technical Reports, Institute for Prospective Technological Studies Digital Economy Working Paper 2013/04, Joint Research Centre, European Commission

music as a substitute for legal purchases. Similarly, it has been found that pirates are heavy legal music consumers.[46]

A slightly older study by Oxera (2011)[47] provides a possible yet partial explanation for the findings in the previous paragraph by listing "Hear before you buy" as one of the four main economic reasons for music piracy. In this case, it is possible that piracy increases legal sales because some people may want to be certain that they like a specific song or album before they purchase it. However, the complete list of reasons for pirating, namely

- Unwillingness to pay,
- Hear before you buy,
- Not wanting a whole album, and
- Unavailable to buy,

looks like a negative substitution effect would prevail. This is because the motives "Unwillingness to pay" and "Not wanting a whole album" suggest that consumers are unlikely to purchase a legal version of a song once they have acquired an illegal one. (Note that the reason "Unavailable to buy" is irrelevant for the question of interest). In other words, the majority of the (relevant) reasons suggest that piracy displaces legal sales, which is consistent with the majority of the literature.

Overall, the evidence for the negative effect of piracy on the music industry is convincing and significant.

[46] The American Assembly (2013) "Copy Culture in the US and Germany", Columbia University and MusicWatch (2016) "Bad Company, You Can't Deny", post based on the MusicWatch (2015), "Badquisition" study

[47] Oxera (2011)" Competing with 'free'? The damages of music piracy" Oxera Agenda October 2011

THE COST OF MUSIC PIRACY IN EUROPE

In May 2016 EUIPO published a report on the cost of music piracy in Europe.[48] Applying different forecasting models to IFPI recorded music sales data for 19 European countries for the period 2005-2014, they considered the differences between predicted and actual sales as "losses" and tried to explain these losses with various explanatory variables including GDP growth, GDP per capita and willingness to pirate music. With this method, they found that in 2014, music piracy:

1. caused a loss of 5.2% of revenue (€170 million) to the recorded music industry in Europe,
2. allowed for effects on other industries, including sales losses to the EU economy were €336 million,
3. caused losses of 2,155 jobs and €63 million in government revenue.

However, IFPI criticized the methodology[49] used by EUIPO on the grounds that

1. the model does not take into account long-term and sustained losses through piracy: Industry revenues were already strongly affected by piracy in 2005 so that losses calculated with the above method cannot estimate the total effect of piracy on revenues
2. calculated losses in each country are constrained by that country's legal revenues in previous years: A country with high legal music revenues therefore can show greater losses than one in which the legal music industry may already have suffered severe damage from piracy.
3. it is not clear whether the variables used by EUIPO (e.g. 'the percentage considering it acceptable to download content from the internet when it is for personal use […]; and the growth rate of the World Bank Index of Control of Corruption'[50]) capture the actual levels of piracy in each country.

In sum, IFPI considers EUIPO's results to be underestimates of the losses actually suffered by the music industry.

4.3.2 Estimating piracy in music

In order to quantify the commercial value of digitally pirated music, we proceed in a similar way as we did for movies. For data reasons, we again favour a bottom-up approach over a top-down approach[51], which means that we multiply the number of illegal music downloads by an average price of recorded music.

The starting point for our calculation is the number of illegal music downloads via BitTorrent networks provided by TECXIPIO. In 2015 they amounted to 2.5 Billion.

[48] EUIPO (2016) "The Economic Cost of IPR Infringement in the Recorded Music Industry"

[49] We received this information in our conversations with IFPI.

[50] EUIPO (2016) "The Economic Cost of IPR Infringement in the Recorded Music Industry", p. 13

[51] Most crucially, we were unable to find a recent and robust estimate of global economic losses due to music piracy. Instead, we have reliable data on the global volume of illegal music downloads (from TECXIPIO) and the prices of different music mediums in the US (from RIAA) so that a bottom-up approach would appear as sufficiently robust.

According to MusicMetric[52], 22% of all BitTorrent music downloads are singles and 78% are albums. Assuming an average of 10 tracks per album, we can calculate 19.7 Billion downloaded **tracks** via BitTorrent networks in 2015.

Although the use of P2P networks has long been the most popular method of unlicensed music acquisition, it is by far not the only one. Over the last decade, the emergence of various new forms of music piracy such as streamripping, the use of mobile apps or downloading from storage lockers has caused a decrease in the prevalence of P2P services. MusicWatch estimates that the number of Americans that use P2P services has decreased from 41 million to 22 million in the period 2004-2015 while the total number of Americans that engage in music piracy of some form has risen to 57 million.[53] Nonetheless, since BitTorrent is particularly well suited (and as shown above primarily used) for downloading whole albums, it still contributes the greatest share of piracy in terms of tracks, namely 72%. The following table displays the most recent estimates by IFPI on the contribution of each of the main piracy areas to overall tracks downloaded globally.

Table 5 Split of music piracy by piracy area (in terms of tracks)

Piracy form	Percentage of overall tracks downloaded
Stream ripping	9%
BitTorrent	72%
Lockers	16%
MP3 sites	3%

Source: IFPI. Data still to be published, but was provided for purposes of this report and is used here with permission of IFPI. Note: 1) The data refers to the 12 months to June 2016. 2) The split excludes P2P activity outside BitTorrent, primarily from the Ares network which is popular in Latin America, and EMule which is popular in Europe. Since these only comprise 1-2% of total music piracy, however, their exclusion can only have marginally affected the above numbers. 3) China is not included in the above split because there is limited information on how exactly the market works. However, since it is the 14th largest music market globally, this should not have significantly affected the above numbers.

Using this information to scale up our above estimate of illegally downloaded tracks via BitTorrent networks, we estimate that there were **27.4 Billion illegally downloaded tracks across all forms of music piracy in 2015.**

In order to get from the total number of illegally downloaded songs to a total commercial value, we again need to multiply by the price of a relevant legal substitute. Unsurprisingly, experts disagree on what this legal substitute could be. On the one hand The American Assembly argues that legal streaming satisfies consumers' demand for cheap, convenient access to music in a similar way as pirated music does.[54] On the other hand, MusicWatch highlights that 'ownership' matters to pirates so that one would expect purchasing a song (digitally or physically) rather than streaming to be a closer substitute to pirating.[55] Because of such ambiguous evidence, we generated a weighted average price across all different forms of legal music consumption (CDs and other physical discs, digital permanent downloads, digital subscriptions and streaming), using sales volumes as weights. These should provide a reasonable proxy for consumers'

[52] MusicMetric (2012) Digital Music Index

[53] http://www.musicwatchinc.com/blog/bad-company-you-cant-deny/

[54] The American Assembly (2013) Copy Culture in the US & Germany

[55] http://www.musicwatchinc.com/blog/bad-company-you-cant-deny/

propensity to engage in the different possible forms of music consumption.[56] The sales volumes as well as the average prices of each music format are obtained from the RIAA 2015 Year-End Industry Shipment and Revenue Statistics.[57] The average price per track in the US is then $1.06.[58]

Multiplying this average price by our estimate of the total number of illegally downloaded tracks in 2015, we find the **value of pirated music in 2015 to be $29 Billion.**

As for movies, it would have been preferable to use global price data instead of US data. However, there are again two reasons why, in the absence of global data, the usage of our chosen US data appears to be a sensible alternative:

1. The US represents the largest market for recorded music in the world with physical and digital recorded music revenues in the US making up 36%[59] of the global market. Hence, any global average price would be dominated by US data, and, by extension, the US can be considered as the single most representative country of global figures.

2. We have performed a sensitivity check based on (less granular) individual country level data of the world's top five music markets by revenue.[60] If we construct a weighted average price of music (spanning digital downloads, physical purchases and streaming) across these five countries and substitute this for the US price in our calculation above, our final estimate of the value of digital music piracy goes down slightly to $25 Billion. This confirms the adequacy of the US data that we have used because it is very close to our original estimate, and the direction of deviation is as expected.[61]

Finally, it should be noted that our approach does not cover music piracy in the form of user uploaded content. A common example of this kind of piracy would be the situation where someone posts a video with infringing content, such as a song for which they don't own the copyright, on YouTube. Typically, this displaces views of other YouTube content, for example the original music video to the song. As this generates fairly low revenue, the damage caused by this type of piracy is likely to be limited. Nonetheless, it is a growing issue and should be an area of future research.

---

[56] Behavioural information as we used to determine movie consumption patterns above would have been preferable. However, such information appeared to be unavailable for music.

[57] RIAA 2015 Year-End Industry Shipment and Revenue Statistics. In the case of streaming we had to combine the revenue figure from RIAA with the estimate of total streams from the 2015 Nielsen Music U.S. Report to derive a per "streaming equivalent track" price. (Streaming equivalent track is our translation from Nielsen's "streaming equivalent album" (where 1,500 streams is equivalent to 1 album.)

[58] Details on the calculation can be found in Table 15, Annex B.

[59] According to figures from the IFPI Global Music Report 2016.

[60] As the data was provided to us by IFPI on a confidential basis, it cannot be displayed here.

[61] The construction of average prices involved dividing revenues by sales volumes in each of the three mentioned categories and bringing in some additional data sources for stream volumes, since IFPI does not record these. Most of these data sources measure something slightly wider than the number of streams that would correspond to the IFPI revenue figures so that they represent overestimates. This means that the resulting prices are skewed downwards slightly so that we expect our final result to be slightly downward biased too.

4.4 Software

$24bn

We estimate that the commercial value of **digital piracy in software** in 2015 was $24 Billion.

4.4.1

In the following, we first give some background on software piracy, reporting research findings from the literature. We then use a "top-down" approach to come up with a value of software piracy.

4.4.2 Overview of research findings

Consumers spent $444 Billion on software around the globe in 2015.[62] And there appears to be a similar shift from physical to digital as has been observed in all media industries over the last decade. To give an example, while physical software sales in the U.S. declined by 13% between 2014 and 2015, global digital video game sales grew by 8%.[63]

Piracy in software has been increasing over the last decade. According to the Business Software Alliance (BSA) the commercial value of unlicensed software installed on computers worldwide rose from $40 Billion in 2006 to $52 Billion in 2015 (with a peak of $63 Billion in the period 2011-2013).[64] The rate of unlicensed software installation (as a percentage of total software installation) in 2015 was as high as 39%.[65]

More evidence for the prevalence of software piracy comes from the 2013 version of Kantar Media's Online Copyright Infringement Tracker prepared for the UK's Office of Communications (Ofcom).[66] According to the study, 20% of internet users in the UK aged 12 and above claim to have consumed pirated software at some point in their lives. 12% admitted to have done so in the past three months. Interestingly, 39% of users who had paid for any computer software in the past three months said they had previously accessed some of it for free. 22% even claimed to have accessed *all* of the products for free before purchasing them. It seems to be an analogue to the "Hear before you buy" motive in music piracy. This means that for some users pirated software is not a substitute for authorised software.

Nonetheless, as in the area of film and music, it is likely that for many users pirated software does constitute a substitute for authorised software and hence harms the software industry by displacing legal sales. Indeed, in 2010 BSA estimated that "reducing the piracy rate for PC software by 10 percentage points in four years would create $142

---

62 The figure is the result of multiplying the size of the global IT industry ($3.8 trillion) by the share of software (12%), both of which are given by CompTIA (2016) IT Industry Outlook 2016 https://www.comptia.org/resources/it-industry-outlook-2016-final

63 CNBC (2016) "Digital gaming sales hit record $61 Billion in 2015: Report", published on 26 January 2016 http://www.cnbc.com/2016/01/26/digital-gaming-sales-hit-record-61-Billion-in-2015-report.html

64 BSA (2010) Eighth Annual BSA Global Software 2010 Piracy Study and BSA (2016) "Seizing Opportunity Through License Compliance" Global Software Survey, May 2016. Note that while the 2006 figure is in 2005 dollars, the 2013 figure is in 2013 dollars, and the 2015 figure in 2015 dollars.

65 BSA (2016) "Seizing Opportunity Through License Compliance" Global Software Survey, May 2016.

66 Kantar Media (2013) Online Copyright Infringement Tracker Annex 1 – Individual content types, Wave 4 (Covering period March – May 2013), prepared for Ofcom

Billion in new economic activity".[67] More than 80% of this activity would be direct benefits to the software industry. Moreover, BSA found that if piracy were to drop at a faster pace, the economic gains would be dramatically higher. The findings of McLennan and Le (2011), though of a more general nature, point in the same direction. Using software piracy data from BSA and IDC's Global Software Piracy Study 2006, they find that a 1% decrease in software piracy is associated with a 0.2% increase in GDP per capita growth.[68]

Besides harming the supply side by causing business losses due to displaced sales, pirated or counterfeit software also has substantial negative consequences on the demand side. When pirating software, and especially when downloading it from the Internet, users incur a high risk of catching malware such as viruses, Trojans[69] or keyloggers.[70] According to IDC (2013) the chance of encountering malware when using counterfeit software is 1/3. The resulting costs are immense. In March 2013 IDC estimated that during the year consumers would waste 1.5 Billion hours dealing with malware from counterfeit software; direct costs to enterprises would amount to $114 Billion.[71]

4.4.3 Estimating piracy in software

For data reasons (particularly the lack of transparency around software prices) our approach to estimating piracy in software differs from the bottom-up approach used for estimating piracy in film and music. This time our starting point is the commonly quoted BSA Global Software Survey, which contains piracy rates and commercial values of unlicensed software in all regions of the world. The difficulty of using these numbers, however, is that they capture all kinds of illicit software acquisition some of which do not fall into the category of digital piracy. One example is the use of physical copies of counterfeit software, which is already captured by the domestic and traded counterfeit and piracy figures in section 3 of this report. Hence we need to "backward engineer" the value of digital software piracy by multiplying the BSA estimates by the share of pirated software that comes from online sources. In the following, we will describe our approach in detail.

The regularly published BSA Global Software Survey quantifies the value of unlicensed software installed on PCs around the globe in a given year. The main inputs of the 2016 edition of the report[72] are a global survey of more than 20,000 computer users carried out by IDC, and a survey of 2,200 IT managers in 22 countries. The surveys are used to determine the volume and type of software installed on home and enterprise computers and PC users' attitudes towards intellectual property and illicit software acquisition.

---

67 BSA (2010) Piracy Impact Study: The Economic Benefits of Reducing Software Piracy

68 McLennan P. G. and Q. V. Le (2011) "The Effects of Intellectual Property Rights Violations on Economic Growth", *Modern Economy,* Vol. 2, pp. 107-113

69 A Trojan is a malicious computer program that is often disguised as legitimate software. Misleading users about its true intent, it hacks into the computer and deletes, blocks, modifies or copies data. It can also be used by hackers for spying, money theft or use of the hacked computer's identity.

70 A Keylogger is a type of software or hardware that records the keys struck on a keyboard, typically without the user being aware of it. It can therefore be used to obtain sensible user data like passwords or PINs.

71 IDC (2013) "The Dangerous World of Counterfeit and Pirated Software", White Paper

72 BSA (2016) "Seizing Opportunity Through License Compliance" Global Software Survey, May 2016

Based on these figures, BSA finds a total worldwide rate of pirated software installation of 39%, corresponding to a value of $52 Billion. This number captures a broad range of software: from operating systems, security packages and business applications to consumer applications like personal finance. It also does not seek to distinguish between the different ways in which such software has been acquired, which means that its coverage is broader than the value of *digital* piracy, which is the specific focus of this chapter.

In order to transform the BSA estimate of total software piracy into a value of digital software piracy, we draw on insights from a 2013 IDC survey:[73] Based on the survey respondents' ranking of top 3 sources of pirated software, IDC estimates that 45% of pirated software comes from online sources such as P2P networks or DDL file sharing systems.[74] Applying this number to scale down the BSA figure we estimate the **value of digital piracy in software to be $24 Billion.**

[73] IDC's (2013) *Dangers of Counterfeit Software Survey* presented in IDC (2013) "The Dangerous World of Counterfeit and Pirated Software", White Paper

[74] DDL stands for "direct download". DDL systems differ from P2P systems in that one downloads the whole file from one server (instead of downloading little pieces from many different sources) and doesn't automatically become a distributer of the file oneself,

EXCURSUS: ESTIMATING DIGITAL PIRACY IN VIDEO GAMES

Another major and increasing area of digital piracy is video games. By way of an exploratory approach, we outline how its commercial value could be estimated in a similar fashion to how we proceeded with digital piracy in music and movies.

In short, such a bottom-up approach would require multiplying the number of illegal games downloads by an appropriate average price of games. The individual steps are outlined below.

1. One could start from the number of BitTorrent downloads, based on worldwide data on games downloads via BitTorrent networks.
2. The figure needs to be scaled up to a total number of illegal downloads, i.e. the number of illegal games downloads via all channels. Here one could draw on insights from Kantar Media's Online Copyright Infringement Tracker.[75] Based on a survey conducted during the period March-May 2013, the study finds that 11% of infringers use BitTorrent services to source pirated computer software. It seems justifiable to assume that this largely holds true for games too.[76] With the additional, conservative assumption that BitTorrent users would not engage in pirating games via any other channels, one can use these 11% to scale up the initial result on the number of BitTorrent downloads.
3. The average price of games in the US is $38.[77] In lack of better data, one could use this as a proxy for the global average price of games.
4. Multiplication of this average price by the quantity of illegally downloaded games yields a total value of digital piracy in games.

Depending on the availability of data, one could proceed in a similar way with piracy in mobile gaming.

4.5 Conclusion and discussion

The following table summarizes the results of our estimations of piracy in the areas movies, music and software.

[75] Kantar Media (2013) Online Copyright Infringement Tracker, Annex 1 – Individual content types, Wave 4 (Covering period March – May 2013), prepared for Ofcom

[76] The study does not separately list BitTorrent for games.

[77] This is the result of dividing the 2013 dollar sales figure of the US computer and video game software industry by the 2013 unit sales figure as recorded by ESA (2014) "Essential Facts about the computer and video game industry", http://www.theesa.com/wp-content/uploads/2014/10/ESA_EF_2014.pdf.

Table 6 Summary of estimates of digital piracy

Result	2015	2022 (forecast)
Estimate of digital piracy in film	$160 Billion	$289-644 Billion
Estimate of digital piracy in music	$29 Billion	$53-117 Billion
Estimate of digital piracy in software	$24 Billion	$42-95 Billion
Estimate of digital piracy in film, music and software	**$213 Billion**	**$384-$856 Billion**

Source: Frontier estimates based on latest data from industry sources (2015)

In summary, we estimate the value of digital piracy in music, movies and software in 2015 to be **$213 Billion**. We project that this value is likely to increase to **$384 - $856 Billion** by 2022. This projection is based on the following assumptions: either (i) that the share of piracy relative to counterfeiting and piracy as a whole remains stable over time; or (ii) that the share of piracy grows in line with projected growth in global IP traffic (The reader is referred to section 6.1 for a fuller discussion).

We consider our bottom-up approach as relatively robust. The TECXIPIO data gives us very reliable estimates of BitTorrent activities worldwide, and multiplication of the number of illegal downloads by a weighted average price is a straight forward and sensible approach to estimating the value of piracy.

Nonetheless, it is not clear how far online activity in places like China or Russia (that are two of the biggest for piracy) can be fully captured even by a BitTorrent-tracker. This suggests (as a first caveat to our approach) that the TECXIPIO figures and, by extension, our estimates may be slight underestimates of the true value of digital piracy.

Moreover, the shares of BitTorrent network activity compared to other forms of digital piracy can change quickly from year to year so that even the usage of the most recent available data (like the 2013 NetNames study) may not be sufficient for capturing the latest behavioural trends in digital piracy. From information from IFPI, we know that the popularity of BitTorrent may have declined a little since 2013. This means that we would have to scale up the TECXIPIO figures by even higher numbers than the NetNames (2013) study suggest to arrive at the total number of illegal movie downloads. Like with the first caveat, this means that our estimates may be slightly lower than the true value of digital piracy.

The third and most significant caveat to our approach is that we construct average prices based on US data. Naturally, global weighted average prices of movies, music and software would have been preferable – however, such estimates are impossible to obtain with the currently existing data. In several places, we have outlined why the US data that we have used is a reasonable proxy. However, it is possible that the results nonetheless differ slightly from the true value of digital piracy. It is not clear in which direction this effect works.

Weighing the above considerations, it seems possible that the commercial value of digital piracy in music, film and software is even higher than we have estimated. In addition, since we have not assessed piracy in a number of areas such as TV-series,

exclusive contents produced by OTT platforms (like Netflix), eBooks, mobile gaming or piracy through user uploaded content, it is most likely that the value of total digital piracy exceeds our estimates by a considerable amount.

5 QUADRANT 4: WIDER ECONOMIC COSTS

5.1 Introduction

As observed in section 2.1, counterfeiting and piracy impose private losses on owners of intellectual property, as well as wider social losses. Specifically, the 2008 OECD report acknowledged that counterfeiting and piracy "can have broader economy-wide effects on trade, foreign investment, employment, innovation, criminality and the environment…and with respect to governments, counterfeiting and piracy have direct effects on tax revenues and government expenditures."

The OECD's work acknowledged the likely significance of these costs. It was not, however, within the scope of their research to attempt to quantify these costs. The purpose of this section is therefore to extend the analysis initiated by the OECD by attempting to quantify these wider economic costs.

The first issue on which we focus is the question of economic growth. More specifically, we wish to examine to what extent an increase in the level of counterfeiting and piracy reduces economic growth. There are several *a priori* reasons that suggest that such illicit activities could reduce economic growth:

- The erosion of intellectual property rights weakens the incentives to innovate. This has a direct impact on well-being by reducing the range of products and services consumers can access, and, in the longer run, by affecting economic growth. The latter effect operates mainly through the links between innovation, technological progress and productivity.
- The substitution of activities that fall under formal frameworks of governance and regulation, by ones that are not subject to such control, can undermine economic growth. This is because of the close links that such "underground" activities have with various forms of criminality make this substitution (i.e. counterfeiting and piracy) a conduit of resources that support the expansion of these criminal activities. The substitution effect can also erode tax revenues and reduce employment, though the extent to which this is true depends on whether other sectors in the legitimate (taxable) economy expand (for example, if consumers reallocate spending to these sectors, of if labour displaced by counterfeiting or piracy in one sector is reallocated to another sector).

In the case of economic growth, the linkages between counterfeiting and piracy are not uncontested. It has been argued for instance, that while these activities may displace legitimate activities in some sectors, consumers may reallocate any savings they make from purchasing counterfeit, but cheaper, goods to other sectors. The argument has also been made that counterfeiting could enable poorer countries to have cheaper access to technology. Finally, the argument is made that the direction of causality flows from growth to counterfeiting and piracy: as countries become richer and have stronger institutions, they are able to enforce IP rights more effectively.

For these reasons, we employ an econometric methodology that examines, on balance, the effects of counterfeiting and piracy on growth, while controlling for the issue of causality and countervailing factors.

Beyond the effects on economic growth, we consider a range of other specific macro-economic effects: effects on employment, effects of tax, and effects on foreign direct investment. We also consider wider social costs, including the effects of crime and health.

5.2 Econometric analysis of impacts on economic growth

In this section we seek to estimate the impact of counterfeiting and piracy on growth rates by testing the relationship between these variables at the country level, and assessing whether higher levels of this activity are associated with reduced growth. This is a 'top-down' approach, as any observed relationship will capture the whole range of different growth impacts, as well any second-round impacts or counteracting effects, although it will not provide detail on the operation of specific impacts. We begin by considering the appropriate indicators for modelling cross-country variation in counterfeiting and piracy, and then measure the impact of the selected indicator with economic growth.

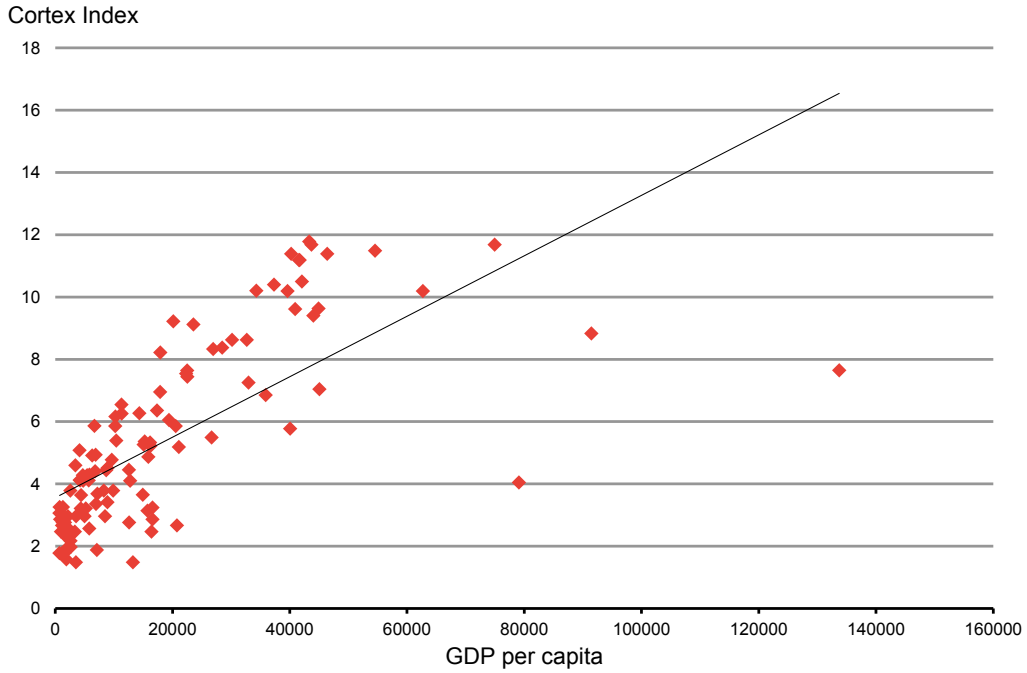
5.2.1 Methodology and approach

Our starting point is the literature that links the enforcement of Intellectual Property Rights (IPRs) to economic performance. One measure of the strength of IPR enforcement is the Cortez Patent Index analysed by Lesser.[78]

Lesser establishes that a variety of scorecard measures of IPR regimes all carry the same information and that it makes little difference which measure is used. His research shows a strong positive relationship between GDP levels and IPR enforcement, as shown in the scatterplot below. Focusing on countries with GDP per capita less than $60,000, a $1000 increase in per capita income is associated with a 0.18 increase in Cortez Index, and GDP explains 78% of the variation in the Cortez Index.

[78] W. Lesser, Measuring Intellectual Property 'Strength' and Effects: An Assessment of Patent Scoring Systems and Causality, 4 J. Bus.Entrepreneurship & L. Iss. 2 (2011)
Available at: http://digitalcommons.pepperdine.edu/jbel/vol4/iss2/4

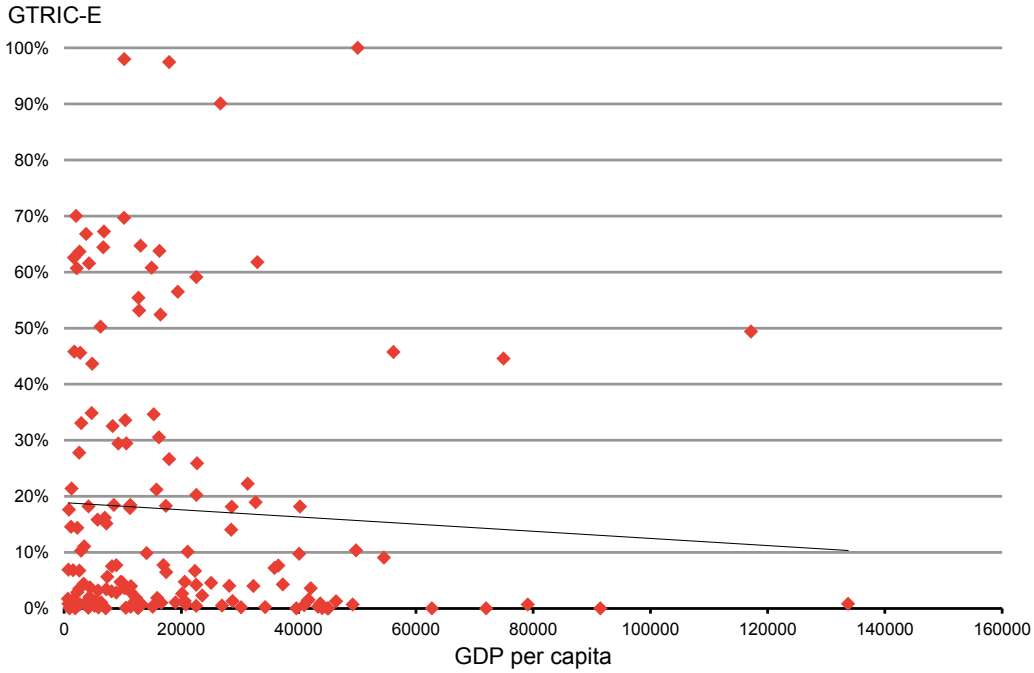
Figure 2. Cortez Index and GDP correlation



Source: Frontier analysis of Lesser (2009) and World Bank data

We then consider whether a similar relationship may hold for indices of counterfeiting as developed by the OECD, such as GTRIC-E. But the relationship between GDP and GTRIC-E is weak. This is apparent from the scatterplot below. In fact, GDP explains only 0.37% of the variation in GTRIC-E. The trend line indicates a slight negative relationship between the two but this effect is not statistically significant.

Figure 3. GTRIC-E and GDP correlation



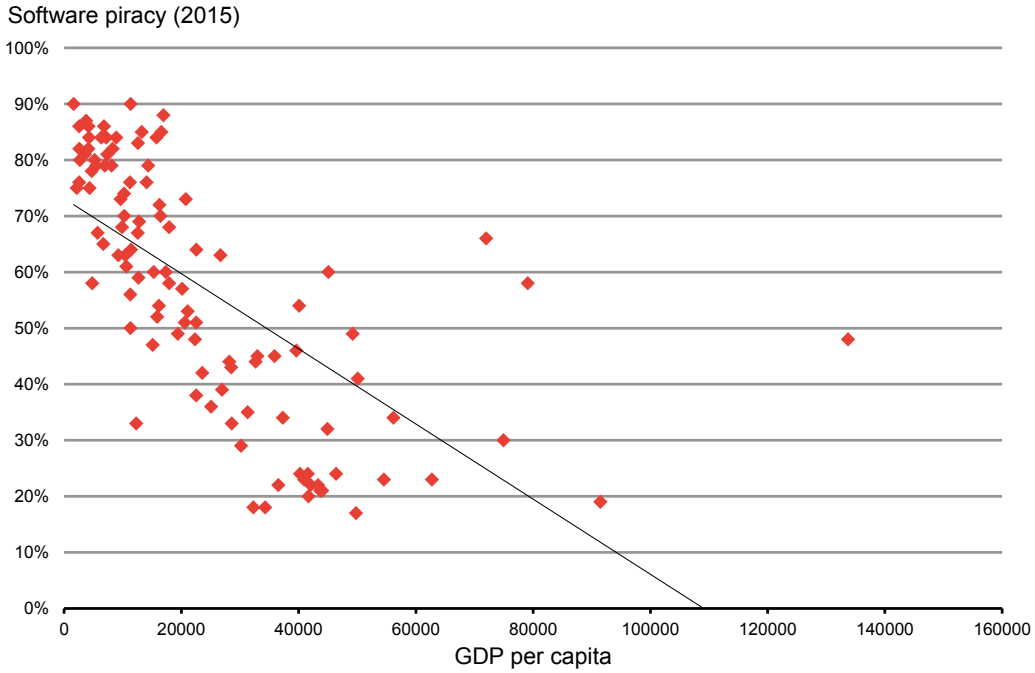
Source: Frontier analysis of OECD and World Bank data

In our view this reflects the particularities of the GTRIC indices, which were developed to estimate an overall global value for piracy and counterfeiting. The work was less concerned with capturing in detail country-by-country variations. Indeed, data and methodological limitations precluded this possibility.

We therefore consider an alternative measure to proxy for country-by-country variation in counterfeiting and piracy. BSA Software Alliance estimates the prevalence of software piracy by country. This is done by comparing legitimate sales of software with the estimated amount of software use by country. The "software load" estimates are based on a global survey of software users and IT managers, assessing the number of computers and amount of software installed by country. This uniform approach applied across countries should give more consistent estimates, with less scope for the measurement error issues than arise in relation to GTRIC.

Software piracy is closely correlated with GDP per capita, as shown in Exhibit 3, below. GDP per capita explains 42% of the variation in piracy rates (68% if countries with GDP in excess of £60,000 per capita are excluded). Software piracy is highly correlated with other intellectual property right enforcement measures, for example explaining 80% of variation in the Cortez index. It is therefore a reasonable proxy for wider IPR infringement including counterfeiting.

Figure 4. Piracy and GDP correlation



Source: Frontier analysis of BSA and World Bank data

Our approach therefore is to estimate the impact of counterfeiting and piracy on growth rates. Specifically, we use the average growth rate from 2009 to 2015. In keeping with the economic theory of growth we control for the level of GDP (log GDP as at 2009), to allow for the possibility that poorer countries grow quicker than richer countries and eventually catch up. We also want to control for various other institutional and policy factors that affect growth, and we do this by incorporating a variable representing the World Bank Ease of Doing Business index.[79] We then explore the effect on economic growth of a percentage point change in piracy rate between 2009 and 2015.[80]

5.2.2 Results

We report the results in the table below. The column headings refer to different specifications of the growth equation that we estimated – one in which we measure the effects of piracy in isolation, and another in which we measure the effects in combination with the Ease of Doing Business index.

[79] For more information on World Bank Ease of Doing Business index, please refer to: http://www.doingbusiness.org/

[80] Although the selected indicator relates specifically to piracy, due to the high correlation of piracy with counterfeiting and other intellectual property right infringement, it is reasonable to infer that these impacts reflect a wider set of activities, rather than piracy in isolation. However, it is not possible to conclude on the relative impacts of different types of infringing activity.

Table 7 Regression of GDP growth on change in piracy

	(1) Piracy	(2) Piracy, EDB
Log GDP	-0.007***	-0.011***
Change in piracy	-0.329***	-0.212***
Change in EDB		0.001***
Constant	0.072***	0.071***
N	109	107
R-squared	0.25	0.32

Source: Frontier analysis of World Bank and BSA data

In all cases, we see a negative impact of piracy on growth. This is consistent with the findings of McLennan and Le (2011).[81] Specific points note are:

- A 1 percentage point increase in piracy reduces growth by between 0.33 and 0.21 percentage points (e.g. from 2% to 1.7% or 1.8%). Applied to nominal GDP forecasts for the OECD as a whole to 2017, **a one (1) percentage point reduction in piracy would be associated with an additional 34 to 54 Billion US dollars.**
- We continue to observe a negative effect of piracy on growth even when we control for the effects of other institutional factors that improve the business climate of a country.

Taken together, the results demonstrate that there are substantial payoffs in terms of economic growth opportunities from investing in actions that lower the incidence of counterfeiting and piracy. In particular, actions to curb counterfeiting and piracy carry their own weight in relation to broader institutional measures to improve the climate for business and investment in a country. Policy decisions and investments to reduce the incidence of counterfeiting and piracy can therefore be seen as valuable extension of broader reform measures that are taken to stimulate economic growth.

[81] Q. Le and P. McLennan, "The Effects of Intellectual Property Rights Violations on Economic Growth," Modern Economy, Vol. 2 No. 2, 2011, pp. 107-113.

5.3 Impacts on displaced economic activity, tax, employment and investment

In this section we consider the effects of international and domestic counterfeiting and piracy on the (i) displacement of economic activity (lost GDP), (ii) uncollected tax losses to government and (iii) displaced or lost employment. Since counterfeit and pirated products displace genuine products, and tax is unlikely to be earned on them, so government tax revenue is reduced. Employment involved in producing the genuine product will also be reduced. We model these impacts by combining (i) estimates of international and domestic counterfeit and pirated goods by country and product, (ii) assumptions on displacement at the product level, and (iii) tax and employment data at the country level.

This approach builds on the methodology developed in our 2009 study.[82] In the 2009 study, industry expert opinion was used to develop assumptions on displacement for specific sectors, and the tax and employment impacts modelled in close detail for UK and Mexico, and then extrapolated to other G20 countries.

Here we extend the 2009 displacement assumptions to cover a much wider range of goods (each 'Comtrade' HS code) and we use the GTRIC estimates of counterfeit prevalence for each country, rather than extrapolate from UK and Mexico. But due to the large number of countries analysed, and their different structures of tax systems, it is not feasible to analyse a country's tax impact in detail. Instead, we use some of the relativities of sales, income, corporation tax and benefits identified in the 2009 study, and apply these to the displacement estimates to derive full at the country level.

This analysis estimates the total amount of genuine economic activity displaced by counterfeit activity[83], and the direct impact on taxes and employment. These impacts are 'gross' in the sense that counterfeit production will also employ labour and may pay some taxes (e.g. where taxed inputs are used). There may also be inter-country effects if, say, counterfeit exports from country A displace genuine exports from country B. While it is difficult to arrive at such net effects, the size of displacement effects indicates the potential distortions arising from counterfeiting, with resources allocated away from efficient and integrated supply chains and into illicit modes of production.

5.3.1 Displacement of genuine products

For this model, we firstly need to estimate the displacement of genuine products. The amount of genuine activity displaced by counterfeits depends on the proportion of consumers that would purchase the genuine product if the counterfeit was unavailable. This is further split-out by whether consumers are knowingly or unknowingly purchasing the counterfeit products, as the displacement propensity may vary for these two groups. Those who knowingly purchase counterfeit products are unlikely to have purchased the

[82] http://www.iccwbo.org/Data/Documents/Bascap/Why-enforce/Deterioration-of-tax-base/Impact-of-Counterfeiting-on-Governments-and-Consumers-Exec-Summary/

[83] This will include physical piracy to the extent to which extent that physical pirated goods appear in the Comtrade data, but not capture displacement due to online piracy.

genuine equivalents, typically purchasing the counterfeit because it has characteristics of the genuine product but is substantially cheaper. By contrast those who were deceived into purchasing the product would be more likely to have purchased the genuine product if the counterfeit was unavailable, so for this group there is a relatively higher propensity for counterfeits to displace genuine products.

The 2009 study developed the assumptions on displacement on the basis of existing national and international research, questionnaire evidence from firms in the sectors concerned, and primary consumer survey evidence commissioned by BASCAP.

The following displacement rates were assumed (same for both UK and Mexico):

Table 8 Displacement rates used in 2009 study

Product	Displacement rate
Leather clothes	57%
Luggage, handbags	57%
Footwear	51%
Perfume	51%
Watches	46%
Jewellery	57%
Other	51%
Food and beverages	95%
Pharmaceuticals	100%
Software	86%

Source: Frontier Economics / BASCAP 2009 study

Note that displacement is generally lower for luxury goods or more 'discretionary' items, for which there is greater scope of undercutting prices of genuine products and boosting sales. By contrast, for more 'commodified' products such as food, drink or pharmaceuticals, it is more likely that the counterfeit does not have the characteristics of the genuine product. For example, counterfeit medicine is unlikely to be as effective as genuine. As a result, displacement rates are higher for these goods.

Based on the above assumptions derived in detail for the 2009 study, we have made the assumptions for each HS code appearing in the Comtrade data, ranging between displacement of 50% and 100%. The displacement rate is assumed to be lowest for goods such as clothing, equipment and perfumes and highest for pharmaceuticals, chemicals and foodstuffs.

Table 9 Displacement assumptions by product category

Product group	HS codes	Displacement assumption
Tobacco	24	50%
Perfume	33	50%
Special fabrics	58	50%
Clothing	61-67	50%
Precious stones and coins	71	50%
Electrical equipment	85	50%
Manufactured equipment and articles	90-96	50%
Art and antiques	97	50%
Raw textiles and leathers	41-43, 50-53	55%
Carpets and knitted fabrics	57,60	60%
Stone, glass, ceramics	68-70	80%
Vehicles	86-89	80%
Foodstuffs	1-23	95%
Rubbers and plastics	34-40	95%
Wood and paper products	44-49	95%
Man-made fibres	54-59	95%
Metal and mineral products	72-83	95%
Chemical and pharmaceutical products	25-32	100%

Source: Extension of Frontier assumptions used in 2009 study

The total amount of activity displaced is a product of the displacement rate, the counterfeiting rate and total consumption. We can therefore estimate total displacement by using current data on counterfeiting rate (from GTRIC), total consumption (ISIC D) and the assumed displacement rates. This suggests that in 2013, between $470bn and $597bn of genuine activity was displaced by counterfeiting (the range depends on assumptions concerning the level of domestic counterfeiting).

Table 10 Displaced activity due to counterfeiting

Type of counterfeiting	**Low domestic scenario**	**High domestic scenario**
International	$313bn	$313bn
Domestic	$157bn	$283bn
Total	**$470bn**	**$597bn**

Source: Frontier analysis of OECD and Comtrade data

5.3.2 Tax and employment impact

The amount of displaced activity feeds through into a number of different impacts – lost business tax (sales tax, corporation tax, excise duty), lost income tax and increased benefit payments to unemployed as a result of displacement. In the 2009 study, these

impacts were modelled in close detail by sector for the UK and Mexico. The most important category of financial impact was in sales tax – representing between 70% and 90% of losses, depending on sector. For the UK, sales tax represented 81% of the overall economic cost, whereas for Mexico it represented 92%.

We calculate sales tax impacts simply by multiplying the amount of displaced activity by the sales tax rate in the consuming country. This suggests that the reduction in sales tax across countries as a result of displacement effects is in the range of $70bn to $89bn per annum.

Table 11 Impact on sales tax revenue as a result of displacement due to counterfeiting

Type of counterfeiting	High domestic scenario	Low domestic scenario
International	$45bn	$45bn
Domestic	$24bn	$44bn
Total	**$70bn**	**$89bn**

Source: Frontier analysis of OECD and Comtrade data

The impacts through other tax channels are much more complicated, as they would depend on each country's tax structure and would need to be modelled on a country-by-country basis.

Given the relativities between sales tax and other tax impacts estimated previously for UK and Mexico, there could be between $8bn and $22bn global reduction in other taxes as a result of displacement effects.[84]

Employment impacts are calculated by dividing through displaced output by GDP per worker, which is calculated at country level from the World Bank WDI dataset and World Economic Outlook data.[85][86] This would suggest gross employment losses in the range of 18m and 23m. Of these, some would quickly find other employment, and others (around 1/3) would be long-term unemployed. [87] In order to translate this into a net employment loss, we need to consider the proportion of displaced workers that would subsequently find other employment, which we assume to be 2/3 of the long-term unemployed. This would give net job losses in the range of 2.0m to 2.6m.

[84] Range depends on level of domestic counterfeiting and assumed ratio of non-sales to sales tax (20:80 or 10:90).

[85] WEO data reports GDP per worker. This is translated into an industry/manufacturing measure using industry share of employment and industry share of GDP reported in WDI. Although it would be desirable to measure lost employment at country-product level, consistent data on GDP per worker by product and country are not available.

[86] An implicit assumption is that the counterfeit and genuine products originate from the same country. In fact there may be considerable displacement effects, e.g. if domestic counterfeits in country A displace imports from country B. Such effects are beyond the scope of this study.

[87] This is calculated using country-level breakdown of unemployment by duration reported by the ILO. Across countries around one third of unemployed are long-term (unemployed for a year or more). We assume of that proportion of long term eventually unemployed finding jobs is 2/3, leaving 1/3 of the long term unemployed without jobs. Hence, net job losses are given by 18m*1/3*1/3 = 2m and 23m*1/3*1/3 = 2.6m

5.3.3 Foreign Direct Investment impact

Lenient IPR enforcement in a country is likely to make firms in IPR-sensitive sectors less eager to invest there. This is because of the vulnerability of proprietary processes to theft, and/ or that infringing products are more likley to displace sales of genuine products. By contrast, enforcing intellectual property rights can stimulate FDI, and through that channel improve welfare in the host country. [88]

A study[89] by the NBER quantifies the impact of IPR enforcement on FDI and through this on exports. The study found that stricter enforcement of IPRs increased exports by up to 20%. For the purposes of our estimation, we take into account the fact that other studies have found that the effects of IPRs on FDI and economic performance may be uneven across countries[90]. Hence, we adopt a more conservative approach regarding the effects of IPRs on FDI and exports. We assume that a country's exports will be 5% lower as a result of lax IPR enforcement, as it is less attractive to locate production of IPR-intensive goods in these countries.

We estimate these FDI impacts by identifying IPR-sensitive sectors and countries with high rates of counterfeiting. We draw on evidence from the European Commission[91] in identifying the IPR-sensitive sectors, which mainly relate to equipment manufacture, pharmaceuticals, chemicals and metallurgy. We define as low IPR countries those with a GTRIC-E score greater than 0.5.

On this basis, the total reduction in FDI is estimated as $111bn, calculated by applying a 5% reduction to Comtrade exports in the relevant sectors and countries. This is associated with lost sales tax of $18bn.

There are also likely to be wider tax impacts (e.g. on corporation tax and excise tax), but these vary according to a country's specific tax regime. In addition, there are likely to be further dynamic impacts on the economy, as there is less exposure to innovation and R&D spill overs that would be brought by FDI.

5.4 Other social impacts

In addition to the effects reported above, various other negative social impacts of counterfeiting and piracy have been documented. The United Nations, for example, finds that these activities have recognised links to organised crime, and have negative

[88] See HitoshinTanaka and Tatsuto Iwaisako (2014), "Intellectual property rights and Foreign Direct Investment: A Welfare analysis", in European Economic Review, Vol. 67, pp 107-124

[89] Intellectual Property Rights, Imitation and Foreign Direct Investment: Theory and Evidence, Lee Branstetter, Raymond Fisman, C. Fritz Foley and Kamal Saggi, Working Paper 13033, National Bureau of Economic Research , April 2007

[90] See notably Mila Kascheeva (2013), "The role of foreign direct investment in the relation between intellectual property and growth", Oxford Economic Papers, Vol. 65 (3):pp 699-720

[91] http://ec.europa.eu/internal_market/intellectual-property/docs/joint-report-epo-ohim-final-version_en.pdf

impacts on health, the environment, and labour conditions.[92] There are also reported links between these activities and terrorism. [93]

The dollar value of these negative impacts is difficult to quantify. We report one attempt at quantification relating to criminality. For other areas, such as health, we present evidence drawn from qualitative assessments and case studies.

5.4.1 Crime

Counterfeiting and piracy are criminal activities in and of themselves. But they also support the further development of criminality by providing crime organisations with funds to support criminal activities more generally. Socials costs reflect increases in the impact of criminality brought about by an increase in counterfeiting. The impacts include the value of lost lives, the costs incurred in anticipation of crime, and the physical and emotional consequences of crime. Estimating these costs require data on how far counterfeiting increases criminality, and the dollar value of the impact of crime.

The 2009 study developed an estimate of the social costs of crime due to counterfeiting by assuming a 1% increase in the crime rate due to counterfeiting, and applying this to other estimates quantifying the value of the cost of crime. Separate valuations were used for the UK and Mexico, [94] and then extrapolated to other countries. Applying this approach, global impacts due to increased criminality are estimated to be in the region of $60bn per annum.

We caution that these results are preliminary. An avenue for further research would be to estimate the impact of counterfeiting on specific forms of criminality, but this would be a daunting empirical task and it may be difficult generalising such results to other countries.

5.4.2 Health impacts

The consumption of counterfeit and pirated goods can have negative effects on health because the products are not subject to the regulatory standards and production norms that govern legitimate goods and services. The problem applies to a range of products. To give an example, it seems likely that a large proportion of deaths through alcohol poisoning in Russia (17,302 in 2012) is caused by counterfeit products, which account for 30-40% of alcoholic beverages in the country.[95]

---

[92] United Nations Office on Drugs and Crime, The Illicit Trafficking of Counterfeit Goods and Transnational Organised Crime.

[93] Gregory F. Treverton, Carl Matthies, Karla J. Cunningham, Jeremiah Goulka, Greg Ridgeway, Anny Wong, (2009) Film Piracy, Organised Crime, and Terrorism, Rand Corporation.

[94] Specifically, we used an estimate provided by the UK Home Office (see Home Office Research Study 217, "The economic and social costs of crime"), which valued the social cost of crime at Euros 80 Billion for the period 1999-2000. This estimate was then revalued to account for a drop in the crime rate since the estimation period, and an increase in prices. For Mexico, the starting point was estimates of crime found in "The Social Costs of Crime in Mexico City and Suburban areas" by R Villoro, George Washington University, G Teruel Universidad Iberoamericana, Estudios Economicos 2003.

[95] Kotelnikova Z. (2014) „Consumption of counterfeit Alcohol in Contemporary Russia: The Role of Cultural and Structural Factors", Basic Research Program, Working Papers, National Research University, Higher School of Economics, https://www.hse.ru/data/2014/08/06/1314159630/47SOC2014.pdf and Bazenkova A. (2015) "Russian

The highest costs, however, likely arise in relation to counterfeit pharmaceuticals and medicine. The WHO estimates that in some developing countries counterfeits comprise between 10-30% of the market value of drug sales.[96] In developed countries the share is much lower (about 1%), but even here the issue seems to be growing as "drug shortages, a long and convoluted supply chain, and Internet pharmacies" facilitate access for counterfeits into the market.[97] The total number of deaths related to counterfeit drugs is hard to determine[98], but Interpol's estimate of more than a million per year gives an idea of the order of magnitude.[99]

Particularly great harm seems to come from fake malaria drugs. A recent study found that in 2013 counterfeit, substandard or degraded anti-malarials contributed to the deaths of more than 120,000 children below 5 in sub-Saharan Africa.[100] The majority of counterfeit drugs comes from China and India,[101] and many traders choose Africa as destination because of relatively open borders and "completely disparate pharmaceutical distribution systems".[102]

Counterfeit pharmaceuticals may contain incorrect dosages of active ingredients, the wrong active ingredient, or no active ingredient at all.[103] In some cases they may have no effect whatsoever, but in other cases they may contain fatal amounts of active ingredients or other toxic chemicals.

Beyond the direct health effects arising from the consumption of counterfeit and pirated foodstuffs or medicines, there will also be substantial indirect effects. These include: loss of household livelihoods when principal wage earners are affected, reduced labour productivity, loss of confidence in health systems, and increased work load for health workers[104]

Government Cracks Down on Counterfeit Alcohol", *The Moscow Times* from 7 October 2015, https://themoscowtimes.com/articles/russian-government-cracks-down-on-counterfeit-alcohol-50131

96 UNODC (2010) „The Globalization of Crime – A Transnational Organized Crime Threat Assessment", http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

97 e.g. Blackstone E. A., Fuhr, J. P and Pociask S. (2014) "The Health and Economic Effects of Counterfeit Drugs", *American Health & Drug Benefits, Vol. 7, No. 4, pp. 216-224,* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4105729/

98 because it is difficult to know with certainty whether it was in fact a fake drug that killed the patient and not, for example, the fact that a good quality drug had been given too late.

99 Natalie Southwick (2013) 'Counterfeit drugs kill 1mn people annually – Interpol!', *Insight Crime* from 24 October 2013, http://www.insightcrime.org/news-briefs/counterfeit-drugs-kill-1-million-annually-interpol

100 Nayyar G. M. L., Breman J. G. and Herrington J. (2015) "The Global Pandemic of Falsified Medicines: Laboratory and Field Innovations and Policy Perspectives", *The American Journal of Tropical Medicine and Hygiene* 15-0221 http://www.ajtmh.org/content/early/2015/04/16/ajtmh.15-0221.full.pdf+html

101 UNODC (2013) „Transnational Organized Crime in West Africa: A Threat Assessment", http://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf, pp. 40-41

102 ibid., p. 43

103 WHO (2016) "Substandard, spurious, falsely labelled, falsified and counterfeit (SSFFC) medical products", Fact sheet, http://www.who.int/mediacentre/factsheets/fs275/en/

104 Robles Y. R., Casauay, J. F. and Bulatao B. P. (2016), "Addressing the Barriers to Effective Monitoring, Reporting and Containment of Spurious/Substandard/Falsely-labelled/Falsified/Counterfeit Medical Products through Sustainable Multi-stakeholder Collaboration and Community/Consumer-based Interventions", A report prepared for the Medicines Transparency Alliance, Philippines, http://www.who.int/medicines/areas/coordination/SSFFC_Report.pdf

5.5 Conclusion

There are substantial wider economic and social costs stemming from counterfeiting and piracy. Indeed, our estimates for displacement effects, employment effects, supressed FDI and crime probably understate the extent of these costs. This is because these estimates do not capture the effects of digital piracy.

Our econometric analysis of the link between piracy and GDP establishes a link between illicit activity and dampened growth, consistent with other empirical studies in this area. Erosion of intellectual property rights is associated with poorer standards of governance and transparency, reducing incentives to invest or innovate, impacting on the long-term growth path of a country. The displacement of genuine activity by illicit activity is also likely to reduce efficiency, as the 'underground' economy is likely to have more irregular supply chains that do not optimally allocate resources. The diversion from genuine to criminal activity reduces government tax revenues and may also have serious consumer impacts due to regulatory non-compliance.

We have modelled a number of these wider social costs in detail using data at the country and product level. The summary estimates of the wider social costs of counterfeiting are shown below. The 2022 forecast is developed by applying projected growth in counterfeiting to the 2013 figures.

Table 12 Summary of estimates of wider impacts of international and domestic counterfeiting

Result	2013	2022 (forecast)
Estimated Displacement of economic activity	$470-$597 Billion	$980-$1244 Billion
Estimated FDI impact	$111 Billion	$231 Billion
Estimated tax loss	$96-$130 Billion	$199-$270 Billion
Estimated costs of crime due to counterfeiting	$60 Billion	$125 Billion
Estimated employment loss (gross)	18-23 million	38-49 million
Estimated employment loss (net)	2-2.6 million	4.2-5.4 million
Estimated value of lost growth (OECD region 2017)	$30-54 Billion	

Source: Frontier estimates

6 CONCLUSIONS

In this section, we project the value of counterfeiting and piracy forward, and summarise our results across the four quadrants.

6.1 Projections of the future incidence of counterfeiting and piracy

We project the estimates forward to 2022 to show how the scale of counterfeiting and piracy may change over time.

$991bn

We forecast that the value of international trade in counterfeit goods could reach $991 Billion by 2022.

First, we project forward the OECD/EUIPO's estimates of international trade in counterfeit and pirated goods to 2022. We forecast an average annual growth rate in trade of counterfeit and pirated goods of 9%.

This projection is estimated using a proxy for growth in future trade volumes. We draw on the World Trade Organisation's estimates of the annual growth rate of global merchandise import volumes, including forecasts to 2017. To forecast beyond 2017, we use the average actual and forecast growth rate as appropriate for 2012-17.

In addition, to account for the growth in counterfeiting and piracy, we use the average annual growth rate in the ratio of customs seizures to real imports in the EU and USA. These grew by 12% on average over 2005-14. Given that some of the growth in the ratio may result from stricter policy and enforcement (leading to an increase in seizures that in the past may entered unchecked), we assume that only half of this growth is the result of increased counterfeiting and piracy.

Using our estimate of the future growth rate of trade in counterfeit and pirated goods, we forecast that the value of trade in counterfeit and pirated goods could reach **$991 Billion** by 2022.

We carry out a similar exercise to illustrate how the size of domestic production and consumption of counterfeit and pirated goods may change over time, projecting our 2013 estimates forward. We forecast an average annual growth rate in domestic production and consumption of counterfeits of 9%.

$524-959bn

We forecast that the value of domestically produced and consumed counterfeit goods could range from $524 - $959 Billion by 2022.

This is estimated by extrapolating from

recent and forecast global GDP growth, as reported by the World Trade Organisation, to estimate annual GDP growth of 2.6% on average. Additionally, we account for growth in counterfeiting and piracy in the same way as in our projections of future trade in counterfeit and pirated goods.

Using this approach, we forecast that the value of domestically produced and consumed counterfeit and pirated goods could range from **$524 - $959 Billion** by 2022. This is a conservative approach to forecasting growth in counterfeiting and piracy. Comparing our preferred estimates of domestic counterfeiting and piracy from 2011-13 suggests an observed annual growth rate of 14%, although some of this change over time could be the result of changes to enforcement policy, or measurement error.

Following our methodology in the previous study, we use two different approaches to project digital piracy into the future.

$384-856bn

We forecast that the value of digital piracy in movies, music and software could range from $384 -$856 Billion by 2022.

- **The first approach assumes that all forms of digital piracy will maintain their respective share of total counterfeiting and piracy over time.** Our findings for 2015 suggest that the ratio of digital piracy to the value of counterfeit and pirated goods calculated in quadrants 1 and 2 lies between 0.20 and 0.25. If this ratio stays the same until 2022, the value of digital piracy will be approximately $384 Billion in 2022, according to our projections for quadrants 1 and 2. Proceeding in the same way on a disaggregated level, digital piracy in film will reach approximately $289 Billion, digital piracy in music $53 Billion and digital piracy in software $42 Billion in 2022. This approach is rather conservative because it does not take into account that internet usage in general and digital media consumption in particular are likely to grow faster over the next couple of years than the non-digital components of the market – as they have done in the past. Giving an example for media, the digital share of total media spending increased from 25.1% in 2008 to 40.1% in 2013 and is projected to rise to 50.4% in 2018[105]. It is likely that this could carry through to the share of digital piracy in total counterfeiting and piracy.
- **The second approach assumes that digital piracy grows proportionally to global IP traffic.** In a comprehensive study[106] Cisco projects global IP traffic to grow at a compound annual growth rate of 22% between 2015 and 2020. If piracy grows at the same speed as IP traffic and if the growth rate stays the same until 2022, all else being equal, the value of digital piracy is expected to reach $856 Billion in 2022 – comprising $644 from digital piracy in film, $117 from digital piracy in music and $95 from digital piracy in software. This approach is supported by one of the headline

[105] McKinsey Global Media Report 2014

[106] Cisco Visual Networking Index: Forecast and Methodology, 2015-2020

results of the NetNames study cited above: 'Internet usage continues to grow at a rapid pace; and with it, so does internet-based infringement.'[107]

Combining these two approaches, we forecast that the value of digital piracy in movies, music and software could reach from $384 - $856 Billion by 2022.

6.2 Projection of wider social and economic costs

As reported in section 5.5, we project changes in wider economic and social costs by applying projected growth in counterfeiting figures to the existing (2013) estimates, and assuming that the costs grow in line with counterfeiting. Based on that approach, we find that:

- Estimated impacts on lost Foreign Direct Investments are $231 Billion
- Estimated tax losses are $199 to $270 Billion
- Estimated costs of crime are $125 Billion

6.3 Summary of results

The analysis presented in this report underscores the magnitude of the policy problem posed by counterfeiting and piracy. Counterfeiting and piracy activities are broad in scope and large in value, and are growing. Using the more robust methodology developed by the OECD, and applying this to more recent data, we find that in 2013, the economic value of counterfeit and pirated products is estimated at between $0.9 Trillion and $1.1 Trillion. Our projections for 2022 show an increase to between $1.9 Trillion to 2.81 Trillion.

Comparing the findings

Comparisons between this report and the one we published in 2011 need to be handled with care because of refinements made to the OECD's methodology.

Nonetheless, it is worthy of a review. In our previous report we projected that the value of counterfeiting and piracy activities would be between $1.2 and 1.8 Trillion in 2015. On the basis of the data and approach followed in this report, we adjusted our base data figures from 2013 to create a 2015-year comparison, and we estimate that in 2015, counterfeiting and piracy stood at between $1.1 Trillion and $1.6 Trillion.

[107] NetNames (2013) „Sizing the piracy universe"

This report also takes a wider, global approach and a much deeper investigation into the broader social economic impacts and finds the losses flowing from these activities are significant. In generating our estimates, we consider four aspects of the economy that are negatively impacted by counterfeiting and piracy: (i) the magnitude of displaced economic activity, (ii) the impact on foreign direct investment, (iv) fiscal costs, and (iv) the economic costs of crime. We arrive at a figure of $737 Billion to $898 Billion for 2013, and projections of between $1.6 Trillion and $1.9 Trillion in 2022. These are non-insignificant costs to the global economy, nearly equal to the economic value of counterfeit and pirated products.

This report also implements recognised methodologies to estimate the foregone growth and development opportunities that arise from counterfeiting and piracy. We estimate that on a global basis, an increase in the incidence of counterfeiting and piracy reduces growth rates by between 0.21 and 0.33 percentage points. For the OECD region, this is worth between $30 and 54 Billion in 2015 alone in foregone growth opportunities.

We also estimate significant employment effects: an estimated 2 to 2.6 million jobs lost globally in 2013, and projected losses of 4.2 to 5.4 million by 2022.

Table 13 Summary of estimates of counterfeiting and piracy

Quadrant	Estimate	2013	2022 (forecast)
1	Total international trade in counterfeit goods	$461 Billion	$991 Billion
2	Total domestic production and consumption of counterfeit goods	$249 - $456Billion	$524 - $959 Billion
3	Digital piracy in film, music and software	$213Billion	$384-856Billion
	- Digital piracy in film	$160 Billion	$289-644 Billion
	- Digital piracy in music	$29 Billion	$53-117 Billion
	- Digital piracy in software	$24 Billion	$42-95 Billion
	Total value of counterfeit and pirated goods	**$923 Billion – 1.13 Trillion**	**$1.90 -$2.81 Trillion**
4	Wider economic and social costs		
	- Displacement of legitimate economic activity	$470-$597 Billion	$980-$1244 Billion
	- Estimated reduction in FDI	$111 Billion	$231 Billion
	- Estimated fiscal losses	$96-$130 Billion	$199-$270 Billion
	- Estimated costs of crime	$60 Billion	$125 Billion
	Total Wider economic and social costs	**$737 Billion-898 Billion**	**$1.54 - $1.87 Trillion**
	Estimated employment losses	**2-2.6 million**	**4.2-5.4 million**
	Foregone economic growth in OECD 2017	**$30 Billion to $54 Billion**	

Source: Frontier estimates based on OECD 2013 data on counterfeiting in international trade, and UN trade and GDP data to derive estimates for domestic production and consumption. Data for Piracy based on latest industry sources (2015).

It is important to continue to highlight the scale of the challenge posed by counterfeiting and piracy globally. We believe that a number of next steps are important, including the following.

- Further research into the prevalence of counterfeiting and piracy of physically traded goods that don't cross borders. Our analysis infers the prevalence of domestically produced and consumed counterfeits using the OECD/EUIPO analysis of internationally traded counterfeits. Further research would help ensure more precise estimates of the scale of domestic counterfeiting in future.
- The digital piracy landscape is changing rapidly. Further data collection and analysis to understand the scale of growing forms of digital piracy (e.g. gaming, copyright infringing user generated content, TV series) would help policymakers to better target digital piracy.

  Further analysis of and improvements to the customs seizures data that underlies the OECD/EUIPO analysis would be beneficial, for example in helping policymakers build up a picture of how prevalence of counterfeiting in different sectors and geographies varies year on year.

As noted at the beginning of this report, measuring the scale of counterfeiting and piracy not only helps us to understand the size of the problem, and the related social costs, but more importantly, it helps inform policymakers. With greater awareness of and appreciation for the enormous size of the problem and the significant impacts of counterfeiting and piracy on consumers, society, government and business, policymakers are better equipped to assign greater priority to fighting these crimes and allocating resources appropriately towards combating counterfeiting and piracy.

ANNEX A CONSTRUCTING AN AVERAGE PRICE OF MOVIES

Table 14 Movie watching behaviour and average prices in the US

Activity	Percentage	Percentage within movie consumption	Price per movie ($)
Watch TV live	34%	n/a	n/a
Play Games owned	12%	n/a	n/a
Subs. Stream TV/Movies	10%	26%	0.51
Watch TV on DVR	8%	n/a	n/a
Watch TV/Movies owned on Disc	7%	18%	4.72
Play Games Online Free	6%	n/a	n/a
Watch TV/Movies free on internet	5%	13%	0
Watch TV/Movies owned Digitally	4%	10%	4.72
Watch TV/Movies rented on disc	4%	10%	4.72
Watch TV on Cable VoD	4%	n/a	n/a
Watch Movies in Theatres	3%	14%	8.43
Play games rented	2%	n/a	n/a
Watch movies rented PP/VOD	1%	5%	0.51
Watch movies rented digitally (1 x Fee)	1%	5%	4.72
Weighted Average Price			**3.35**

Source : ***Percentages*** *calculated from Nielsen (2015) Home Entertainment Consumer Trends – Digital Transition Tracker Report, accessible at http://www.slideshare.net/JonathanBlumKurtz/home-entertaiment-consumer-trends; conversion to* ***Percentages within movie consumption*** *carried out by using the shares of TV and movies within Netflix consumption from Nielsen (2014)The Digital Consumer, accessible at http://www.slideshare.net/tinhanhvy/the-digital-consumer-report-2014-nielsen;* ***Price per Movie*** *(dollars) from http://money.cnn.com/2012/03/22/technology/streaming-movie-sales/ (average prices of 'physical' and 'online' movies in the US in 2012, which we have attributed to the above categories as appropriate) and http://www.the-numbers.com/market/ (average cinema ticket in the US in 2015); Percentages within movie consumption were taken as weights for calculating the weighted average price*

ANNEX B CONSTRUCTING AN AVERAGE PRICE OF MUSIC

Table 15 Music shipments, revenues and prices in the US

Format	Dollar value ($millions)	Units (million)	Tracks (million)	Average price per track ($)
Total physical retail units				
CD	1520.8	122.9	1229.0	1.24
CD Single	1.2	0.4	0.8	1.50
LP/EP	416.2	16.9	84.5	4.93
Vinyl Single	6.1	0.5	1.0	6.10
Music Video	73.2	3.3	33.0	2.22
DVD Audio	5.4	0.2	2.0	2.70
Digital Permanent Download				
Download Single	1226.9	1021	1021.0	1.20
Download Album	1090.7	109.4	1094.0	1.00
Kiosk	3.7	2.2	17.6	0.21
Music Video	6.4	3.2	3.2	2.00
Digital Subscription & Streaming				
Tracks	1604	317200	2114.7	0.76
Weighted Average Price				**1.06**

Source: ***Dollar values*** *and* ***units*** *(except for streamed tracks) are taken from RIAA 2015 Year-End Industry Shipment and Revenue Statistics; streamed track units are "streaming equivalent tracks" (where 150 streams are equivalent to one track) based on the streams figure given by the 2015 Nielsen Music U.S. Report; conversion to* ***Tracks*** *was done making assumptions on the number of tracks per medium;* ***Average prices per track*** *are calculated by dividing the Dollar value by the number of tracks; track numbers were taken as weights for calculating the weighted average price*

Note: We use stream equivalent tracks instead of streams because as people listen to the same stream multiple times, counting each of these as one track would decrease the average price below a reasonable level.

frontier
economics

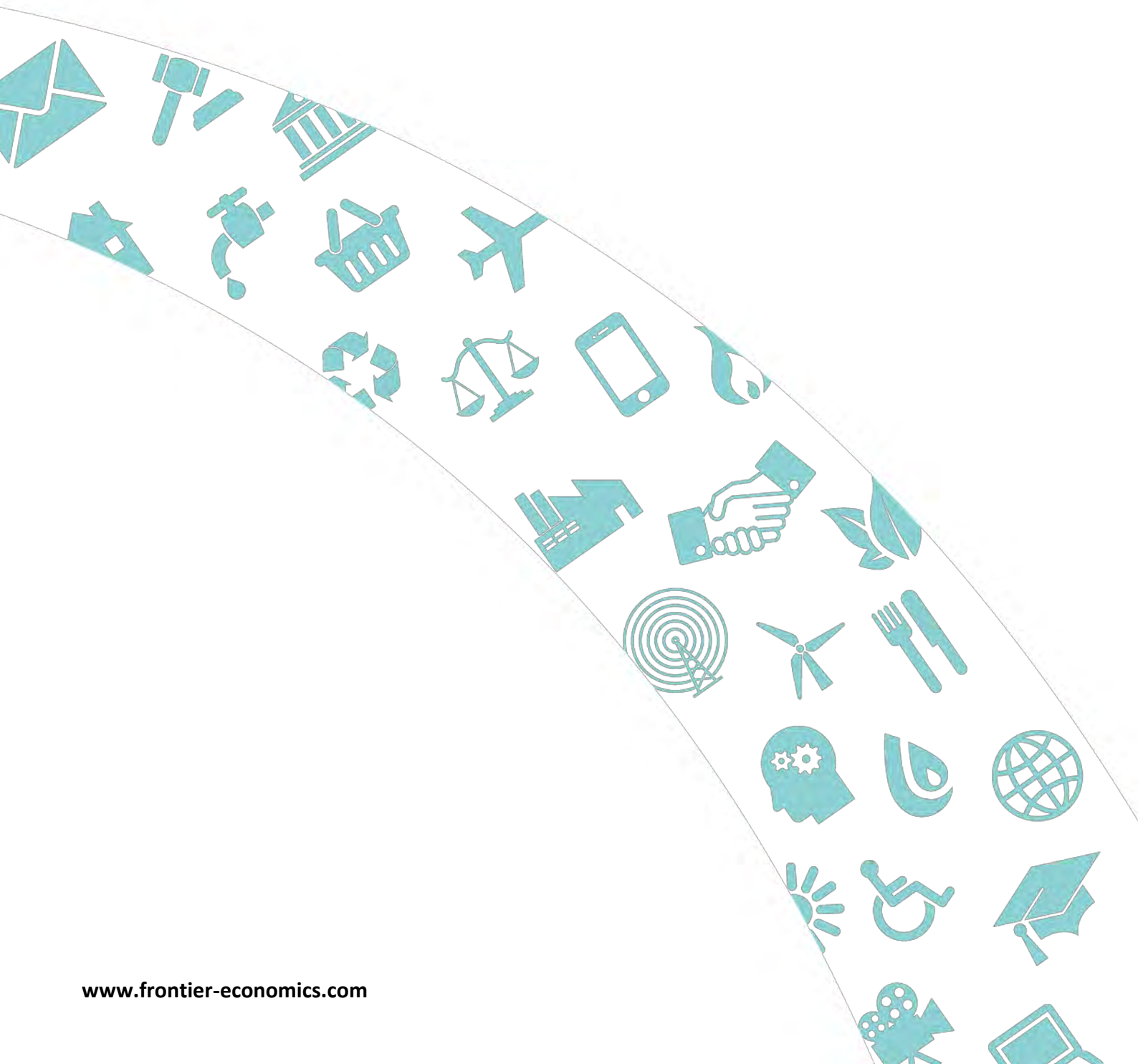


EXHIBIT 4

2013 Registrar Accreditation Agreement

1. **Registrar Accreditation Agreement**
2. **RDDS Accuracy Program Specification**
3. **Registration Data Directory Services (RDDS) Specification**
4. **Consensus and Temporary Policy Specification**
5. **Specification on Privacy and Proxy Registrations**
6. **Data Retention Specification**
7. **Registrar Information Specification**
8. **Additional Registrar Operation Specification**
9. **Registrants' Benefits and Responsibilities Specification**
10. **Logo License Specification**
11. **Compliance Certificate**
12. **Transition Addendum**

Registrar Accreditation Agreement

This REGISTRAR ACCREDITATION AGREEMENT (this "Agreement") is by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), and shall be deemed made on _____, at Los Angeles, California, USA.

1. DEFINITIONS. For purposes of this Agreement, the following definitions shall apply:

1.1 "Account Holder" means the person or entity that is paying for the Registered Name or otherwise controls the management of the registered name, when that person or entity is not the Registered Name Holder.

1.2 "Accredited" or "Accreditation" means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of Registrar Services.

1.3 "Affiliate" means a person or entity that, directly or indirectly, through one or more intermediaries, Controls, is controlled by, or is under common control with, the person or entity specified.

1.4 "Affiliated Registrar" is another Accredited registrar that is an Affiliate of Registrar.

1.5 "Applicable Registrar Family" means, with respect to Affiliated Registrars, such Affiliated Registrar as a group.

1.6 "Consensus Policy" has the meaning set forth in the Consensus Policies and Temporary Policies Specification attached hereto.

1.7 "Control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise.

1.8 "DNS" refers to the Internet domain-name system.

1.9 The "Effective Date" is _____.

1.10 The "Expiration Date" is _____.

1.11 "gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN pursuant to a registry agreement that is in full force and effect, other than any country code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

1.12 "gTLD Zone-File Data" means all data contained in a DNS zone file for the registry, or for any subdomain for which Registry Services are provided and that contains Registered Names, as provided to nameservers on the Internet.

1.13 "Illegal Activity" means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.

1.14 "Personal Data" refers to data about any identified or identifiable natural person.

1.15 "RDDS Accuracy Program Specification" means the RDDS Accuracy Program Specification attached hereto, as updated from time to time in accordance with this Agreement.

1.16 "RDDS Specification" means the Registration Data Directory Services Specification attached hereto, as updated from time to time in accordance with this Agreement.

1.17 "Registered Name" refers to a domain name within the domain of a gTLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

1.18 "Registered Name Holder" means the holder of a Registered Name.

1.19 The word "registrar," when appearing without an initial capital letter, refers to a person or entity that contracts with Registered Name Holders and with a Registry Operator and collects registration data about the Registered Name Holders and submits registration information for entry in the Registry Database.

1.20 "Registrar Approval" means the receipt of either of the following approvals:

1.20.1 The affirmative approval of Applicable Registrars accounting for 90% of the Total Registered Names Under Management by the Applicable Registrars; provided that, for purposes of calculating the Total Registered Names Under Management by Applicable Registrars, the Total Registered Names Under Management by each Applicable Registrar Family shall not exceed the Total Registered Names Under Management of the Applicable Registrar Family that is the fifth largest Applicable Registrar Family (measured by number of Registered Names Under Management), both for purposes of the numerator and the denominator; or

1.20.2 The affirmative approval of 50% plus one of the Applicable Registrars that participate in the process to approve or disapprove (i.e. vote for or against, but not abstain or otherwise fail to vote) a proposed amendment under Section 6, and the affirmative approval of Applicable Registrars accounting for 66.67% of the Total Registered Names Under Management by all Applicable Registrars; provided that, for purposes of calculating the Total Registered Names Under Management by Applicable Registrars, the Total Registered Names Under Management by each Applicable Registrar Family shall not exceed the total Registered Names Under Management of the Applicable Registrar Family that is the fifth largest Applicable Registrar Family (measured by number of Registered Names Under Management), both for purposes of the numerator and the denominator. An example of these calculations is set forth in Appendix 1 attached hereto.

1.21 "Registrar Services" means the services subject to this Agreement provided by a registrar in connection with a gTLD, and includes contracting with Registered Name Holders, collecting registration data about the Registered Name Holders, and submitting registration information for entry in the Registry Database.

1.22 "Registry Data" means all Registry Database data maintained in electronic form, and shall include gTLD Zone-File Data, all data used to provide Registry Services and submitted by registrars in electronic form, and all other data used to provide Registry Services concerning particular domain name registrations or nameservers maintained in electronic form in a Registry Database.

1.23 "Registry Database" means a database comprised of data about one or more DNS domain names within the domain of a registry that is used to generate either DNS resource records that are published authoritatively or responses to domain-name availability lookup requests or RDDS queries, for some or all of those names.

1.24 A "Registry Operator" is the person or entity then responsible, in accordance with an agreement between ICANN (or its assignee) and that person or entity (those persons or entities) or, if that agreement is terminated or expires, in accordance with an agreement between the US Government and that person or entity (those persons or entities), for providing Registry Services for a specific gTLD.

1.25 "Registry Services," with respect to a particular gTLD, shall have the meaning defined in the agreement between ICANN and the Registry Operator for that gTLD.

1.26 A "Reseller" is a person or entity that participates in Registrar's distribution channel for domain name registrations (a) pursuant to an agreement, arrangement or understanding with Registrar or (b) with Registrar's actual knowledge, provides some or all Registrar Services, including collecting registration data about Registered Name Holders, submitting that data to Registrar, or facilitating the entry of the registration agreement between Registrar and the Registered Name Holder.

1.27 "Restricted Amendment" means (i) an amendment of the Consensus Policies and Temporary Policies Specification or (ii) the term of this Agreement as specified in Section 5.1, as such term may be extended pursuant to Section 5.2.

1.28 A Registered Name is "sponsored" by the registrar that placed the record associated with that registration into the registry. Sponsorship of a registration may be changed at the express direction of the Registered Name Holder or, in the event a registrar loses Accreditation, in accordance with then-current ICANN Specifications and Policies.

1.29 "Specifications and/or Policies" include Consensus Policies, Specifications (such as the RDDS Accuracy Program Specification) referenced in this Agreement, and any amendments, policies, procedures, or programs specifically contemplated by this Agreement or authorized by ICANN's Bylaws.

1.30 "Term of this Agreement" begins on the Effective Date and continues to the earlier of (a) the Expiration Date, or (b) termination of this Agreement.

1.31 "Total Registered Names Under Management" means the total number of Registered Names sponsored by all Applicable Registrars as reflected in the latest monthly reports submitted to ICANN by Registrars.

1.32 "WHOIS Accuracy Program Specification" refers to the RDDS Accuracy Program Specification and is included in this Section 1 for purposes of external documents linking to this Agreement using this definition.

1.33 "Working Group" means representatives of the Applicable Registrars and other members of the community that the Registrar Stakeholder Group appoints, from time to time, to serve as a working group to consult on amendments to the Applicable Registrar Agreements (excluding bilateral amendments pursuant to Section 6.9).

2. ICANN OBLIGATIONS.

2.1 Accreditation. During the Term of this Agreement and subject to the terms and conditions of this Agreement, Registrar is hereby Accredited by ICANN to act as a registrar (including to insert and renew registration of Registered Names in the Registry Database) for gTLDs.

2.2 Registrar Use of ICANN Name, Website and Trademarks. ICANN hereby grants to Registrar a non-exclusive, worldwide, royalty-free license during the Term of this Agreement (a) to state that it is Accredited by ICANN as a registrar for gTLDs, and (b) to link to pages and documents within the ICANN website. Subject to the terms and conditions set forth in the Logo License Specification attached hereto, ICANN hereby grants to Registrar a non-exclusive, worldwide right and license to use the Trademarks (as defined in the Logo License Specification). No other use of ICANN's name, website or Trademarks is licensed hereby. This license may not be assigned or sublicensed by Registrar to any other party, including, without limitation, any Affiliate of Registrar or any Reseller.

2.3 General Obligations of ICANN. With respect to all matters that impact the rights, obligations, or role of Registrar, ICANN shall during the Term of this Agreement:

2.3.1 exercise its responsibilities in an open and transparent manner;

2.3.2 not unreasonably restrain competition and, to the extent feasible, promote and encourage robust competition;

2.3.3 not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and not single out Registrar for disparate treatment unless justified by substantial and reasonable cause; and

2.3.4 ensure, through its reconsideration and independent review policies, adequate appeal procedures for Registrar, to the extent it is adversely affected by ICANN standards, policies, procedures or practices.

2.4 Use of ICANN Accredited Registrars. In order to promote competition in the registration of domain names, and in recognition of the value that ICANN-Accredited registrars bring to the Internet community, ICANN has ordinarily required gTLD registries under contract with ICANN to use ICANN-Accredited registrars, and ICANN will during the course of this agreement abide by any ICANN adopted Specifications or Policies requiring the use of ICANN-Accredited registrars by gTLD registries.

3. REGISTRAR OBLIGATIONS.

3.1 Obligations to Provide Registrar Services. During the Term of this Agreement, Registrar agrees that it will operate as a registrar for one or more gTLDs in accordance with this Agreement.

3.2 Submission of Registered Name Holder Data to Registry. During the Term of this Agreement:

3.2.1 As part of its registration of Registered Names in a gTLD, Registrar shall submit to, or shall place in the Registry Database operated by, the Registry Operator for the gTLD the following data elements:

3.2.1.1 The name of the Registered Name being registered;

3.2.1.2 The IP addresses of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.2.1.3 The corresponding names of those nameservers;

3.2.1.4 Unless automatically generated by the registry system, the identity of Registrar;

3.2.1.5 Unless automatically generated by the registry system, the expiration date of the registration; and

3.2.1.6 Any other data the Registry Operator requires be submitted to it.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.2.1.1 through 3.2.1.6 stated above for all purposes under this Agreement but only with respect to that particular gTLD. When seeking approval for alternative required data elements, the data elements set forth in Subsections 3.2.1.1 through 3.2.1.6 should be considered suggested minimum requirements.

3.2.2 Within seven (7) days after receiving any updates from the Registered Name Holder to the data elements listed in Subsections 3.2.1.2, 3.1.2.3, and 3.2.1.6 for any Registered Name that Registrar sponsors, Registrar shall submit the updated data elements to, or shall place those elements in the Registry Database operated by, the relevant Registry Operator.

3.2.3 In order to allow reconstitution of the Registry Database in the event of an otherwise unrecoverable technical failure or a change in the designated Registry Operator, within ten (10) days of any such request by ICANN, Registrar shall submit an electronic database containing the data elements listed in Subsections 3.2.1.1 through 3.2.1.6 for all active records in the registry sponsored by Registrar, in a format specified by ICANN, to the Registry Operator for the appropriate gTLD.

3.3 Public Access to Data on Registered Names. During the Term of this Agreement:

3.3.1 At its expense, Registrar shall provide an RDAP Directory Service (as defined in the RDDS Specification) (accessible via both IPv4 and IPv6) providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar in any gTLD. Until otherwise specified by a Consensus Policy, such data shall consist of the following elements as contained in Registrar's database:

3.3.1.1 The name of the Registered Name;

3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;

3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);

3.3.1.4 The original creation date of the registration;

3.3.1.5 The expiration date of the registration;

3.3.1.6 The name and postal address of the Registered Name Holder;

3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and

3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede Subsections 3.3.1.1 through 3.3.1.8 stated above for all purposes under this Agreement but only with respect to that particular gTLD.

3.3.2 Upon receiving any updates to the data elements listed in Subsections 3.3.1.2, 3.3.1.3, and 3.3.1.5 through 3.3.1.8 from the Registered Name Holder, Registrar shall promptly update its database used to provide the public access described in Subsection 3.3.1.

3.3.3 Registrar may subcontract its obligation to provide the public access described in Subsection 3.3.1 and the updating described in Subsection 3.3.2, provided that Registrar shall remain fully responsible for the proper provision of the access and updating.

3.3.4 Registrar shall abide by any Consensus Policy that requires registrars to cooperatively implement a distributed capability that provides query-based RDDS search functionality across all registrars. If the RDDS service implemented by registrars does not in a reasonable time provide reasonably robust, reliable, and convenient access to accurate and up-to-date data, Registrar shall abide by any Consensus Policy requiring Registrar, if reasonably determined by ICANN to be necessary (considering such possibilities as remedial action by specific registrars), to supply data from Registrar's database to facilitate the development of a centralized RDDS database for the purpose of providing comprehensive Registrar RDDS search capability.

3.3.5 In providing query-based public access to registration data as required by Subsections 3.3.1 and 3.3.4, Registrar shall not impose terms and conditions on use of the data provided, except as permitted by any Specification or Policy established by ICANN. Unless and until ICANN establishes a different Consensus Policy, Registrar shall permit use of data it provides in response to queries for any lawful purposes except to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-

Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.

3.3.6 In the event that ICANN determines, following analysis of economic data by an economist(s) retained by ICANN (which data has been made available to Registrar), that an individual or entity is able to exercise market power with respect to registrations or with respect to registration data used for development of value-added products and services by third parties, Registrar shall provide third-party bulk access to the data subject to public access under Subsection 3.3.1 under the following terms and conditions:

3.3.6.1 Registrar shall make a complete electronic copy of the data available at least one (1) time per week for download by third parties who have entered into a bulk access agreement with Registrar.

3.3.6.2 Registrar may charge an annual fee, not to exceed US$10,000, for such bulk access to the data.

3.3.6.3 Registrar's access agreement shall require the third party to agree not to use the data to allow, enable, or otherwise support any marketing activities, regardless of the medium used. Such media include but are not limited to e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts.

3.3.6.4 Registrar's access agreement shall require the third party to agree not to use the data to enable high-volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.

3.3.6.5 Registrar's access agreement must require the third party to agree not to sell or redistribute the data except insofar as it has been incorporated by the third party into a value-added product or service that does not permit the extraction of a substantial portion of the bulk data from the value-added product or service for use by other parties.

3.3.7 To comply with applicable statutes and regulations and for other reasons, ICANN may adopt a Consensus Policy establishing limits (a) on the Personal Data concerning Registered Names that Registrar may make available to the public through a public-access service described in this Subsection 3.3 and (b) on the manner in which Registrar may make such data available. Registrar shall comply with any such Consensus Policy.

3.3.8 Registrar shall meet or exceed the requirements set forth in the RDDS Specification.

3.3.9 Until the WHOIS Services Sunset Date (as defined in the RDDS Specification), Registrar shall, at its expense, provide web-based WHOIS and, with respect to any

gTLD operating a "thin" registry, a port 43 WHOIS service (each accessible via both IPv4 and IPv6) providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar in any gTLD. Until otherwise specified by a Consensus Policy or a Temporary Policy, such data shall consist of at least the elements described in Subsection 3.3.1.1 through 3.3.1.8 as contained in Registrar's database and in the format set forth in Subsection 1.4 of the RDDS Specification.

3.4 Retention of Registered Name Holder and Registration Data.

3.4.1 For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time:

3.4.1.1 the data specified in the Data Retention Specification attached hereto for the period specified therein;

3.4.1.2 The data elements listed in Subsections 3.3.1.1 through 3.3.1.8;

3.4.1.3 the name and (where available) postal address, e-mail address, voice telephone number, and fax number of the billing contact;

3.4.1.4 any other Registry Data that Registrar has submitted to the Registry Operator or placed in the Registry Database under Subsection 3.2; and

3.4.1.5 the name, postal address, e-mail address, and voice telephone number provided by the customer of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates in connection with each registration. Effective on the date that ICANN fully implements a Proxy Accreditation Program established in accordance with Section 3.14, the obligations under this Section 3.4.1.5 will cease to apply as to any specific category of data (such as postal address) that is expressly required to be retained by another party in accordance with such Proxy Accreditation Program.

3.4.2 During the Term of this Agreement and for two (2) years thereafter, Registrar (itself or by its agent(s)) shall maintain the following records relating to its dealings with the Registry Operator(s) and Registered Name Holders:

3.4.2.1 In electronic form, the submission date and time, and the content, of all registration data (including updates) submitted in electronic form to the Registry Operator(s);

3.4.2.2 In electronic, paper, or microfilm form, all written communications constituting registration applications, confirmations, modifications, or terminations and related correspondence with Registered Name Holders, including registration contracts; and

3.4.2.3 In electronic form, records of the accounts of all Registered Name Holders with Registrar.

3.4.3 During the Term of this Agreement and for two (2) years thereafter, Registrar shall make the data, information and records specified in this Section 3.4 available for inspection and copying by ICANN upon reasonable notice. In addition, upon reasonable notice and request from ICANN, Registrar shall deliver copies of such data, information and records to ICANN in respect to limited transactions or circumstances that may be the subject of a compliance-related inquiry; provided, however, that such obligation shall not apply to requests for copies of Registrar's entire database or transaction history. Such copies are to be provided at Registrar's expense. In responding to ICANN's request for delivery of electronic data, information and records, Registrar may submit such information in a format reasonably convenient to Registrar and acceptable to ICANN so as to minimize disruption to Registrar's business. In the event Registrar believes that the provision of any such data, information or records to ICANN would violate applicable law or any legal proceedings, ICANN and Registrar agree to discuss in good faith whether appropriate limitations, protections, or alternative solutions can be identified to allow the production of such data, information or records in complete or redacted form, as appropriate. ICANN shall not disclose the content of such data, information or records except as expressly required by applicable law, any legal proceeding or Specification or Policy.

3.4.4 Notwithstanding any other requirement in this Agreement or the Data Retention Specification, Registrar shall not be obligated to maintain records relating to a domain registration beginning on the date two (2) years following the domain registration's deletion or transfer away to a different registrar.

3.5 Rights in Data. Registrar disclaims all rights to exclusive ownership or use of the data elements listed in Subsections 3.2.1.1 through 3.2.1.3 for all Registered Names submitted by Registrar to the Registry Database for, or sponsored by Registrar in, each gTLD for which it is Accredited. Registrar does not disclaim rights in the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and Subsections 3.3.1.3 through 3.3.1.8 concerning active Registered Names sponsored by it in each gTLD for which it is Accredited, and agrees to grant non-exclusive, irrevocable, royalty-free licenses to make use of and disclose the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 for the purpose of providing a service or services (such as a RDDS service under Subsection 3.3.4) providing interactive, query-based public access. Upon a change in sponsorship from Registrar of any Registered Name in each gTLD for which it is Accredited, Registrar acknowledges that the registrar gaining sponsorship shall have the rights of an owner to the data elements listed in Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 concerning that Registered Name, with Registrar also retaining the rights of an owner in that data. Nothing in this Subsection prohibits Registrar from (1) restricting bulk public access to data elements in a manner consistent with this Agreement and any Specifications or Policies or (2) transferring rights it claims in data elements subject to the provisions of this Subsection 3.5.

3.6 Data Escrow. During the Term of this Agreement, on a schedule, under the terms, and in the format specified by ICANN, Registrar shall submit an electronic copy of the data described in Subsections 3.4.1.2 through 3.4.1.5 to ICANN or, at Registrar's election and at its expense, to a reputable escrow agent mutually approved by Registrar and ICANN, such approval also not to be unreasonably withheld by either party. The data shall be held under an agreement among Registrar, ICANN, and the escrow agent (if any) providing that (1) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete, consistent, and in proper format, until released to ICANN; (2) the data shall be released from escrow upon expiration without renewal or termination of this Agreement; and (3) ICANN's rights under the escrow agreement shall be assigned with any assignment of this Agreement. The escrow shall provide that in the event the escrow is released under this Subsection, ICANN (or its assignee) shall have a non-exclusive, irrevocable, royalty-free license to exercise (only for transitional purposes) or have exercised all rights necessary to provide Registrar Services.

3.7 Business Dealings, Including with Registered Name Holders.

3.7.1 In the event ICANN adopts a Specification or Policy that is supported by a consensus of ICANN-Accredited registrars as reflected in the Registrar Stakeholder Group (or any successor group), establishing or approving a Code of Conduct for ICANN-Accredited registrars, Registrar shall abide by that Code of Conduct.

3.7.2 Registrar shall abide by applicable laws and governmental regulations.

3.7.3 Registrar shall not represent to any actual or potential Registered Name Holder that Registrar enjoys access to a registry for which Registrar is Accredited that is superior to that of any other registrar Accredited for that registry.

3.7.4 Registrar shall not activate any Registered Name unless and until it is satisfied that it has received a reasonable assurance of payment of its registration fee. For this purpose, a charge to a credit card, general commercial terms extended to creditworthy customers, or other mechanism providing a similar level of assurance of payment shall be sufficient, provided that the obligation to pay becomes final and non-revocable by the Registered Name Holder upon activation of the registration.

3.7.5 At the conclusion of the registration period, failure by or on behalf of the Registered Name Holder to consent that the registration be renewed within the time specified in a second notice or reminder shall, in the absence of extenuating circumstances, result in cancellation of the registration by the end of the auto-renew grace period (although Registrar may choose to cancel the name earlier).

3.7.5.1 Extenuating circumstances are defined as: UDRP action, valid court order, failure of a Registrar's renewal process (which does not include failure of a registrant to respond), the domain name is used by a nameserver that provides DNS service to third-parties (additional time may be required to migrate the records managed by the nameserver), the registrant is subject to

bankruptcy proceedings, payment dispute (where a registrant claims to have paid for a renewal, or a discrepancy in the amount paid), billing dispute (where a registrant disputes the amount on a bill), domain name subject to litigation in a court of competent jurisdiction, or other circumstance as approved specifically by ICANN.

3.7.5.2 Where Registrar chooses, under extenuating circumstances, to renew a domain name without the explicit consent of the registrant, the registrar must maintain a record of the extenuating circumstances associated with renewing that specific domain name for inspection by ICANN consistent with clauses 3.4.2 and 3.4.3 of this registrar accreditation agreement.

3.7.5.3 In the absence of extenuating circumstances (as defined in Section 3.7.5.1 above), a domain name must be deleted within 45 days of either the registrar or the registrant terminating a registration agreement.

3.7.5.4 Registrar shall provide notice to each new registrant describing the details of their deletion and auto-renewal policy including the expected time at which a non-renewed domain name would be deleted relative to the domain's expiration date, or a date range not to exceed ten (10) days in length. If a registrar makes any material changes to its deletion policy during the period of the registration agreement, it must make at least the same effort to inform the registrant of the changes as it would to inform the registrant of other material changes to the registration agreement (as defined in clause 3.7.7 of the registrars accreditation agreement).

3.7.5.5 If Registrar operates a website for domain name registration or renewal, details of Registrar's deletion and auto-renewal policies must be clearly displayed on the website.

3.7.5.6 If Registrar operates a website for domain registration or renewal, it should state, both at the time of registration and in a clear place on its website, any fee charged for the recovery of a domain name during the Redemption Grace Period.

3.7.5.7 In the event that a domain which is the subject of a UDRP dispute is deleted or expires during the course of the dispute, the complainant in the UDRP dispute will have the option to renew or restore the name under the same commercial terms as the registrant. If the complainant renews or restores the name, the name will be placed in Registrar HOLD and Registrar LOCK status, the RDDS contact information for the registrant will be removed, and the RDDS entry will indicate that the name is subject to dispute. If the complaint is terminated, or the UDRP dispute finds against the complainant, the name will be deleted within 45 days. The registrant retains the right under the existing redemption grace period provisions to recover

the name at any time during the Redemption Grace Period, and retains the right to renew the name before it is deleted.

3.7.6 Registrar shall not insert or renew any Registered Name in any gTLD registry in a manner contrary to (i) any Consensus Policy stating a list or specification of excluded Registered Names that is in effect at the time of insertion or renewal, or (ii) any list of names to be reserved from registration as required by the specific Registry Operator for which Registrar is providing Registrar Services.

3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12, and which agreement shall otherwise set forth the terms and conditions applicable to the registration of a domain name sponsored by Registrar. The Registered Name Holder with whom Registrar enters into a registration agreement must be a person or legal entity other than Registrar, provided that Registrar may be the Registered Name Holder for domains registered for the purpose of conducting its Registrar Services, in which case Registrar shall submit to the provisions set forth in Subsections 3.7.7.1 through 3.7.7.12 and shall be responsible to ICANN for compliance with all obligations of the Registered Name Holder as set forth in this Agreement and Specifications and Policies. Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the registration agreement between Registrar and any Registered Name Holder that relate to implementing the requirements of Subsections 3.7.7.1 through 3.7.7.12 or any Consensus Policy.

3.7.7.1 The Registered Name Holder shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.

3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.

3.7.7.3 Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for

providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it discloses the current contact information provided by the licensee and the identity of the licensee within seven (7) days to a party providing the Registered Name Holder reasonable evidence of actionable harm.

3.7.7.4 Registrar shall provide notice to each new or renewed Registered Name Holder stating:

3.7.7.4.1 The purposes for which any Personal Data collected from the applicant are intended;

3.7.7.4.2 The intended recipients or categories of recipients of the data (including the Registry Operator and others who will receive the data from Registry Operator);

3.7.7.4.3 Which data are obligatory and which data, if any, are voluntary; and

3.7.7.4.4 How the Registered Name Holder or data subject can access and, if necessary, rectify the data held about them.

3.7.7.5 The Registered Name Holder shall consent to the data processing referred to in Subsection 3.7.7.4.

3.7.7.6 The Registered Name Holder shall represent that notice has been provided equivalent to that described in Subsection 3.7.7.4 to any third-party individuals whose Personal Data are supplied to Registrar by the Registered Name Holder, and that the Registered Name Holder has obtained consent equivalent to that referred to in Subsection 3.7.7.5 of any such third-party individuals.

3.7.7.7 Registrar shall agree that it will not process the Personal Data collected from the Registered Name Holder in a way incompatible with the purposes and other limitations about which it has provided notice to the Registered Name Holder in accordance with Subsection 3.7.7.4 above.

3.7.7.8 Registrar shall agree that it will take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

3.7.7.9 The Registered Name Holder shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of

the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party.

3.7.7.10 For the adjudication of disputes concerning or arising from use of the Registered Name, the Registered Name Holder shall submit, without prejudice to other potentially applicable jurisdictions, to the jurisdiction of the courts (1) of the Registered Name Holder's domicile and (2) where Registrar is located.

3.7.7.11 The Registered Name Holder shall agree that its registration of the Registered Name shall be subject to suspension, cancellation, or transfer pursuant to any Specification or Policy, or pursuant to any registrar or registry procedure not inconsistent with any Specification or Policy, (1) to correct mistakes by Registrar or the Registry Operator in registering the name or (2) for the resolution of disputes concerning the Registered Name.

3.7.7.12 The Registered Name Holder shall indemnify and hold harmless the Registry Operator and its directors, officers, employees, and agents from and against any and all claims, damages, liabilities, costs, and expenses (including reasonable legal fees and expenses) arising out of or related to the Registered Name Holder's domain name registration.

3.7.8 Registrar shall comply with the obligations specified in the RDDS Accuracy Program Specification. In addition, notwithstanding anything in the RDDS Accuracy Program Specification to the contrary, Registrar shall abide by any Consensus Policy requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

3.7.9 Registrar shall abide by any Consensus Policy prohibiting or restricting warehousing of or speculation in domain names by registrars.

3.7.10 Registrar shall publish on its website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification attached hereto and shall not take any action inconsistent with the corresponding provisions of this Agreement or applicable law.

3.7.11 Registrar shall make available a description of the customer service handling processes available to Registered Name Holders regarding Registrar Services, including a description of the processes for submitting complaints and resolving disputes regarding the Registrar Services.

3.7.12 Nothing in this Agreement prescribes or limits the amount Registrar may charge Registered Name Holders for registration of Registered Names.

3.8 Domain-Name Dispute Resolution. During the Term of this Agreement, Registrar shall have in place a policy and procedures for resolution of disputes concerning Registered Names. Until ICANN adopts an alternative Consensus Policy or other Specification or Policy with respect to the resolution of disputes concerning Registered Names, Registrar shall comply with the Uniform Domain Name Dispute Resolution Policy ("UDRP") identified on ICANN's website (https://www.icann.org/consensus-policies), as may be modified from time to time. Registrar shall also comply with the Uniform Rapid Suspension ("URS") procedure or its replacement, as well as with any other applicable dispute resolution procedure as required by a Registry Operator for which Registrar is providing Registrar Services.

3.9 Accreditation Fees. As a condition of Accreditation, Registrar shall pay Accreditation fees to ICANN. These fees consist of yearly and variable fees.

3.9.1 Registrar shall pay ICANN a yearly Accreditation fee in an amount established by the ICANN Board of Directors, in conformity with ICANN's bylaws and articles of incorporation. This yearly Accreditation fee shall not exceed US$4,000. Payment of the yearly fee shall be due within thirty (30) days after invoice from ICANN, provided that Registrar may elect to pay the yearly fee in four (4) equal quarterly installments.

3.9.2 Registrar shall pay the variable Accreditation fees established by the ICANN Board of Directors, in conformity with ICANN's bylaws and articles of incorporation, provided that in each case such fees are reasonably allocated among all registrars that contract with ICANN and that any such fees must be expressly approved by registrars accounting, in the aggregate, for payment of two-thirds of all registrar-level fees. Registrar shall pay such fees in a timely manner for so long as all material terms of this Agreement remain in full force and effect, and notwithstanding the pendency of any dispute between Registrar and ICANN.

3.9.3 For any payments thirty (30) days or more overdue, Registrar shall pay interest on late payments at the rate of 1.5% per month or, if less, the maximum rate permitted by applicable law from later of the date of the invoice or the date the invoice is sent pursuant to Section 7.6 of this Agreement. On reasonable notice given by ICANN to Registrar, accountings submitted by Registrar shall be subject to verification by an audit of Registrar's books and records by an independent third-party designated by ICANN that shall preserve the confidentiality of such books and records (other than its findings as to the accuracy of, and any necessary corrections to, the accountings).

3.9.4 The Accreditation fees due under this Agreement are exclusive of tax. All taxes, duties, fees and other governmental charges of any kind (including sales, turnover, services, use and value-added taxes) that are imposed by or under the

authority of any government or any political subdivision thereof on the Accreditation fees for any services, software and/or hardware shall be borne by Registrar and shall not be considered a part of, a deduction from, or an offset against such Accreditation fees. All payments due to ICANN shall be made without any deduction or withholding on account of any tax, duty, charge, or penalty except as required by applicable law, in which case, the sum payable by Registrar from which such deduction or withholding is to be made shall be increased to the extent necessary to ensure that, after making such deduction or withholding, ICANN receives (free from any liability with respect thereof) a net sum equal to the sum it would have received but for such deduction or withholding being required.

3.10 Insurance. Registrar shall maintain in force commercial general liability insurance or similar liability insurance as specified by ICANN with policy limits of at least US$500,000 covering liabilities arising from Registrar's registrar business during the Term of this Agreement.

3.11 Obligations of Registrars under common controlling interest. Registrar shall be in breach of this Agreement if:

3.11.1 ICANN terminates an Affiliated Registrar's accreditation agreement with ICANN (an "Affiliate Termination");

3.11.2 Affiliated Registrar has not initiated arbitration challenging ICANN's right to terminate the Affiliated Registrar's accreditation agreement under Section 5.8 of this Agreement, or has initiated such arbitration and has not prevailed;

3.11.3 the Affiliate Termination was the result of misconduct that materially harmed consumers or the public interest;

3.11.4 a second Affiliated Registrar has pursued, after the Affiliate Termination, the same course of conduct that resulted in the Affiliate Termination; and

3.11.5 ICANN has provided Registrar with written notice that it intends to assert the provisions of this Section 3.11 with respect to Registrar, which notice shall identify in reasonable detail the factual basis for such assertion, and Registrar has failed to cure the impugned conduct within fifteen (15) days of such notice.

3.12 Obligations Related to Provision of Registrar Services by Third Parties. Registrar is responsible for the provision of Registrar Services for all Registered Names that Registrar sponsors being performed in compliance with this Agreement, regardless of whether the Registrar Services are provided by Registrar or a third party, including a Reseller. Registrar must enter into written agreements with all of its Resellers that enable Registrar to comply with and perform all of its obligations under this Agreement. In addition, Registrar must ensure that:

3.12.1 Its Resellers do not display the ICANN or ICANN-Accredited Registrar logo, or otherwise represent themselves as Accredited by ICANN, unless they have written permission from ICANN to do so.

3.12.2 Any registration agreement used by reseller shall include all registration agreement provisions and notices required by the ICANN Registrar Accreditation Agreement and any ICANN Consensus Policies, and shall identify the sponsoring registrar or provide a means for identifying the sponsoring registrar, such as a link to the ICANN Registration data lookup tool (https://lookup.icann.org).

3.12.3 Its Resellers identify the sponsoring registrar upon inquiry from the customer.

3.12.4 Its Resellers comply with any ICANN-adopted Specification or Policy that establishes a program for accreditation of individuals or entities who provide proxy and privacy registration services (a "Proxy Accreditation Program"). Among other features, the Proxy Accreditation Program may require that: (i) proxy and privacy registration services may only be provided in respect of domain name registrations by individuals or entities Accredited by ICANN pursuant to such Proxy Accreditation Program; and (ii) Registrar shall prohibit Resellers from knowingly accepting registrations from any provider of proxy and privacy registration services that is not Accredited by ICANN pursuant the Proxy Accreditation Program. Until such time as the Proxy Accreditation Program is established, Registrar shall require Resellers to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.12.5 Its Resellers' customers are provided with a link to an ICANN webpage detailing registrant educational information, as detailed in subsection 3.16 below.

3.12.6 In the event Registrar learns that a Reseller is causing Registrar to be in breach of any of the provisions of this Agreement, Registrar shall take reasonable steps to enforce its agreement with such Reseller so as to cure and prevent further instances of non-compliance.

3.12.7 Its Resellers shall publish on their website(s) and/or provide a link to the Registrants' Benefits and Responsibilities Specification attached hereto and shall not take any action inconsistent with the corresponding provisions of this Agreement or applicable law.

Registrar shall use commercially reasonable efforts to enforce compliance with the provisions of the agreement between Registrar and any Reseller that relate to the provisions of Registrar Services.

3.13 Registrar Training. Registrar's primary contact as identified in Subsection 7.6 below or designee (so long as the designee is employed by Registrar or an Affiliated Registrar) shall complete a training course covering registrar obligations under ICANN policies and agreements. The course will be provided by ICANN at no expense to Registrar, and shall be available in an online format.

3.14 Obligations Related to Proxy and Privacy Services. Registrar agrees to comply with any ICANN-adopted Specification or Policy that establishes a Proxy Accreditation Program. Registrar also agrees to reasonably cooperate with ICANN in the development of such program. Until such time as the Proxy Accreditation Program is established, Registrar agrees to comply with the Specification on Privacy and Proxy Registrations attached hereto.

3.15 Registrar Self-Assessment and Audits. Registrar shall complete and deliver to ICANN on a schedule and in the form specified by ICANN from time to time in consultation with registrars a Registrar self-assessment. Registrar shall complete and deliver to ICANN within twenty (20) days following the end of each calendar year, in a form specified by ICANN a certificate executed by the president, chief executive officer, chief financial officer or chief operating officer (or their equivalents) of Registrar certifying compliance with the terms and conditions of this Agreement. ICANN may from time to time (not to exceed twice per calendar year) conduct, or engage a third party to conduct on its behalf, contractual compliance audits to assess compliance by Registrar with the terms and conditions of this Agreement. Any audits pursuant to this Section 3.15 shall be tailored to achieve the purpose of assessing compliance, and ICANN will (a) give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested by ICANN, and (b) use commercially reasonable efforts to conduct such audit in such a manner as to not unreasonably disrupt the operations of Registrar. As part of such audit and upon request by ICANN, Registrar shall timely provide all responsive documents, data and any other information necessary to demonstrate Registrar's compliance with this Agreement. Upon no less than ten (10) days' notice (unless otherwise agreed to by Registrar), ICANN may, as part of any contractual compliance audit, conduct site visits during regular business hours to assess compliance by Registrar with the terms and conditions of this Agreement. ICANN shall not disclose Registrar confidential information gathered through such audits except as required by applicable law, legal proceedings, or as expressly permitted by any Specification or Policy (including ICANN's Documentary Information Disclosure Policy, as such policy may be amended from time to time); provided, however, that, except as required by applicable law or legal proceedings, ICANN shall not release any information that Registrar has marked as, or has otherwise designated in writing to ICANN as, a "confidential trade secret," "confidential commercial information" or "confidential financial information" of Registrar. If any applicable law, legal proceeding or Specification or Policy permits such disclosure, ICANN will provide Registrar no less than fifteen (15) days' notice of its intent to disclose such information, unless such notice is prohibited by law or legal proceeding. Such notice shall include to whom and in what manner ICANN plans to disclose such information.

3.16 Link to Registrant Educational Information. ICANN has published an educational webpage summarizing the terms of the Registrar Accreditation Agreement and related Consensus Policies (as of the date of this Agreement, located at: https://www.icann.org/resources/pages/benefits-2013-09-16-en). Registrar shall provide a link to such webpage on any website it may operate for domain name registration or renewal clearly displayed to its Registered Name Holders at least as clearly as its links to

policies or notifications required to be displayed under ICANN Consensus Policies. ICANN may, in consultation with registrars, update the content and/or URL for this website.

3.17 Registrar Contact, Business Organization and Officer Information. Registrar shall provide to ICANN and maintain accurate and current information as specified in the Registrar Information Specification to this Agreement. In addition, Registrar shall publish on each website through which Registrar provides or offers Registrar Services the information specified as requiring such publication in the Registrar Information Specification. Registrar shall notify ICANN within five (5) days of any changes to such information and update Registrar's website(s) within twenty (20) days of any such changes.

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.3 Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

3.19 Additional Technical Specifications to Implement IPV6, DNSSEC and IDNs. Registrar shall comply with the Additional Registrar Operations Specification attached hereto.

3.20 Notice of Bankruptcy, Convictions and Security Breaches. Registrar will give ICANN notice within seven (7) days of (i) the commencement of any of the proceedings referenced in Section 5.5.8. (ii) the occurrence of any of the matters specified in Section 5.5.2 or Section 5.5.3 or (iii) any unauthorized access to or disclosure of registrant account

information or registration data. The notice required pursuant to Subsection (iii) shall include a detailed description of the type of unauthorized access, how it occurred, the number of registrants affected, and any action taken by Registrar in response.

3.21 Obligations of Registrars Affiliated with Registry Operators. In the event Registrar is Affiliated with any Registry Operator or back-end registry operator (an "Affiliated Relationship") during the Term of this Agreement, Registrar shall comply with all ICANN Specifications and Policies that may be developed from time to time with respect to such Affiliated Relationships, and will notify ICANN within thirty (30) days of the occurrence of the event that created the Affiliate relationship (e.g., the closing of any merger, acquisition or other transaction, or the execution of any agreement, in each case, giving rise to such Affiliated Relationship).

3.22 Cooperation with Emergency Registry Service Providers. In the event that ICANN transitions the operation of a registry for a gTLD in which Registrar sponsors Registered Names to an emergency registry service provider, Registrar shall cooperate in all reasonable respects with such emergency registry service provider, including by entering into a registry-registrar agreement with such provider necessary to effect the transition and by providing all Registered Name Holder data reasonably requested by such emergency operator for the purpose of facilitating an efficient transition of the registry for the gTLD.

4. PROCEDURES FOR ESTABLISHMENT OR REVISION OF SPECIFICATIONS AND POLICIES.

4.1 Compliance with Consensus Policies and Temporary Policies. During the Term of this Agreement, Registrar shall comply with and implement all Consensus Policies and Temporary Policies in existence as of the Effective Date found at https://www.icann.org/consensus-policies, and as may in the future be developed and adopted in accordance with the ICANN Bylaws, provided such future Consensus Policies and Temporary Policies are adopted in accordance with the procedures and relate to those topics and subject to those limitations set forth in the Consensus Policies and Temporary Policies Specification to this Agreement.

5. TERM, TERMINATION AND DISPUTE RESOLUTION.

5.1 Term of Agreement. This Agreement shall be effective on the Effective Date and shall have an initial term running until the Expiration Date, unless sooner terminated.

5.2 Renewal. This Agreement and Registrar's Accreditation will be renewed for successive periods of five (5) years upon the Expiration Date and the expiration of each successive five-year term thereafter under the terms and conditions of this Agreement, unless:

5.2.1 at the time of such renewal, Registrar no longer meets the ICANN registrar Accreditation criteria then in effect;

5.2.2 Registrar is not in compliance with its obligations under this Agreement at the time of the Expiration Date or at the expiration of any successive five (5) year term thereafter;

5.2.3 Registrar has been given notice by ICANN of three (3) or more material breaches of this Agreement within the two (2) years preceding the Expiration Date or the date of expiration of any successive five (5) year term thereafter; or

5.2.4 this Agreement has terminated prior to the Expiration Date or the expiration date of any successive five (5) year term thereafter.

In the event Registrar intends to renew this Agreement pursuant to this Section 5.2, Registrar shall provide ICANN written notice thereof during the period that is no more than ninety (90) days and no less than sixty (60) days prior to the Expiration Date and each successive five (5) year term thereafter. The provision of such notice shall not be a condition to renewal hereunder. Pursuant to its customary practices (as may be modified by ICANN), ICANN will provide notice to Registrar of the Expiration Date and the date of expiration of any subsequent term hereunder.

5.3 Right to Substitute Updated Agreement. In the event that, during the Term of this Agreement, ICANN adopts a revised form Registrar accreditation agreement (the "Updated RAA"), Registrar (provided it has not received (i) a notice of breach that it has not cured or (ii) a notice of termination or suspension of this Agreement under this Section 5) may elect, by giving ICANN written notice, to enter into the Updated RAA. In the event of such election, Registrar and ICANN shall as soon as practicable enter into the Updated RAA for the term specified in the Updated RAA, and this Agreement will be deemed terminated.

5.4 Termination of Agreement by Registrar. This Agreement may be terminated before its expiration by Registrar by giving ICANN thirty (30) days written notice. Upon such termination by Registrar, Registrar shall not be entitled to any refund of fees paid to ICANN pursuant to this Agreement.

5.5 Termination of Agreement by ICANN. This Agreement may be terminated before its expiration by ICANN in any of the following circumstances:

5.5.1 There was a material misrepresentation, material inaccuracy, or materially misleading statement in Registrar's application for Accreditation or renewal of Accreditation or any material accompanying the application.

5.5.2 Registrar:

5.5.2.1 is convicted by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is judged by a court of competent jurisdiction to have:

5.5.2.1.1 committed fraud,

5.5.2.1.2 committed a breach of fiduciary duty, or

5.5.2.1.3 with actual knowledge (or through gross negligence) permitted Illegal Activity in the registration or use of domain names or in the provision to Registrar by any Registered Name Holder of inaccurate registration data; or

5.5.2.1.4 failed to comply with the terms of an order issued by a court of competent jurisdiction relating to the use of domain names sponsored by Registrar;

or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing; or

5.5.2.2 is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others; or

5.5.2.3 is the subject of a non-interlocutory order issued by a court or arbitral tribunal, in each case of competent jurisdiction, finding that Registrar has, directly or through an Affiliate, committed a specific violation(s) of applicable national law or governmental regulation relating to cybersquatting or its equivalent; or

5.5.2.4 is found by ICANN, based on its review of the findings of arbitral tribunals, to have been engaged, either directly or through its Affiliate, in a pattern and practice of trafficking in or use of domain names identical or confusingly similar to a trademark or service mark of a third party in which the Registered Name Holder has no rights or legitimate interest, which trademarks have been registered and are being used in bad faith.

5.5.3 Registrar knowingly employs any officer that is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) days of Registrar's knowledge of the foregoing; or any member of Registrar's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Registrar's board of directors or similar governing body within thirty (30) days of Registrar's knowledge of the foregoing.

5.5.4 Registrar fails to cure any breach of this Agreement within twenty-one (21) days after ICANN gives Registrar notice of the breach.

5.5.5 Registrar fails to comply with a ruling granting specific performance under Sections 5.7 or 7.1.

5.5.6 Registrar has been in fundamental and material breach of its obligations under this Agreement at least three (3) times within a twelve (12) month period.

5.5.7 Registrar continues acting in a manner that ICANN has reasonably determined endangers the stability or operational integrity of the Internet after receiving three (3) days' notice of that determination.

5.5.8 (i) Registrar makes an assignment for the benefit of creditors or similar act; (ii) attachment, garnishment or similar proceedings are commenced against Registrar, which proceedings are a material threat to Registrar's ability to provide Registrar Services for gTLDs, and are not dismissed within sixty (60) days of their commencement; (iii) a trustee, receiver, liquidator or equivalent is appointed in place of Registrar or maintains control over any of Registrar's property; (iv) execution is levied upon any property of Registrar, (v) proceedings are instituted by or against Registrar under any bankruptcy, insolvency, reorganization or other laws relating to the relief of debtors and such proceedings are not dismissed within thirty (30) days of their commencement, or (vi) Registrar files for protection under the United States Bankruptcy Code, 11 U.S.C. Section 101 et seq., or a foreign equivalent or liquidates, dissolves or otherwise discontinues its operations.

5.6 Termination Procedures. This Agreement may be terminated in circumstances described in Subsections 5.5.1 through 5.5.6 above only upon fifteen (15) days written notice to Registrar (in the case of Subsection 5.5.4 occurring after Registrar's failure to cure), with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of termination under this Agreement. This Agreement may be terminated immediately upon notice to Registrar in circumstances described in Subsections 5.5.7 and 5.5.8.

5.7 Suspension.

5.7.1 Upon the occurrence of any of the circumstances set forth in Section 5.5, ICANN may, in ICANN's sole discretion, upon delivery of a notice pursuant to Subsection 5.7.2, elect to suspend Registrar's ability to create or sponsor new Registered Names or initiate inbound transfers of Registered Names for any or all gTLDs for a period of up to a twelve (12) months following the effectiveness of such suspension. Suspension of a Registrar does not preclude ICANN's ability to issue a notice of termination in accordance with the notice requirements of Section 5.6.

5.7.2 Any suspension under Subsections 5.7.1 will be effective upon fifteen (15) days written notice to Registrar, with Registrar being given an opportunity during that time to initiate arbitration under Subsection 5.8 to determine the appropriateness of suspension under this Agreement.

5.7.3 Upon suspension, Registrar shall notify users, by posting a prominent notice on its web site, that it is unable to create or sponsor new gTLD domain name registrations or initiate inbound transfers of Registered Names. Registrar's notice shall include a link to the notice of suspension from ICANN.

5.7.4 If Registrar acts in a manner that ICANN reasonably determines endangers the stability or operational integrity of the Internet and upon notice does not immediately cure, ICANN may suspend this Agreement for five (5) working days pending ICANN's application for more extended specific performance or injunctive relief under Subsection 7.1. Suspension of the Agreement under this Subsection may, at ICANN's sole discretion, preclude Registrar from (i) providing Registration Services for gTLDs delegated by ICANN on or after the date of delivery of such notice to Registrar and (ii) creating or sponsoring new Registered Names or initiating inbound transfers of Registered Names for any gTLDs. Registrar must also post the statement specified in Subsection 5.7.3.

5.8 Resolution of Disputes Under this Agreement. Subject to the limitations set forth in Section 6 and Section 7.4, disputes arising under or in connection with this Agreement, including (1) disputes arising from ICANN's failure to renew Registrar's Accreditation and (2) requests for specific performance, shall be resolved in a court of competent jurisdiction or, at the election of either party, by an arbitration conducted as provided in this Subsection 5.8 pursuant to the International Arbitration Rules of the American Arbitration Association ("AAA"). The arbitration shall be conducted in English and shall occur in Los Angeles County, California, USA. Except as set forth in Section 7.4.5, there shall be one (1) arbitrator agreed by the parties from a list of AAA arbitrators, or if parties do not agree on an arbitrator within fifteen (15) days of the AAA request that the parties designate an arbitrator, the AAA shall choose and appoint an arbitrator, paying due regard to the arbitrator's knowledge of the DNS. The parties shall bear the costs of the arbitration in equal shares, subject to the right of the arbitrator to reallocate the costs in their award as provided in the AAA rules. The parties shall bear their own attorneys' fees in connection with the arbitration, and the arbitrator may not reallocate the attorneys' fees in conjunction with their award. The arbitrator shall render its decision within ninety (90) days of the conclusion of the arbitration hearing. In the event Registrar initiates arbitration to contest the appropriateness of termination of this Agreement by ICANN pursuant to Section 5.5 or suspension of Registrar by ICANN pursuant to Section 5.7.1, Registrar may at the same time request that the arbitration panel stay the termination or suspension until the arbitration decision is rendered. The arbitration panel shall order a stay: (i) upon showing by Registrar that continued operations would not be harmful to consumers or the public interest, or (ii) upon appointment by the arbitration panel of a qualified third party to manage the operations of Registrar until the arbitration decision is rendered. In furtherance of sub-clause (ii) above, the arbitration panel is hereby granted all necessary authority to appoint a qualified third-party to manage the operations of Registrar upon Registrar's request and if the panel deems it appropriate. In selecting the third-party manager, the arbitration panel shall take into consideration, but shall not be bound by, any expressed preferences of Registrar. Any order granting a request for a stay must be issued within fourteen (14) days after the filing of the arbitration. If an order granting a request

for a stay is not issued within fourteen (14) days, ICANN has the right to proceed with the termination of this Agreement pursuant to Section 5.5 or suspension of Registrar pursuant to Section 5.7.1. In the event Registrar initiates arbitration to contest an Independent Review Panel's decision under Subsection 4.3.3 sustaining the ICANN Board of Director's determination that a specification or policy is supported by consensus, Registrar may at the same time request that the arbitration panel stay the requirement that it comply with the policy until the arbitration decision is rendered, and that request shall have the effect of staying the requirement until the decision or until the arbitration panel has granted an ICANN request for lifting of the stay. In all litigation involving ICANN concerning this Agreement (whether in a case where arbitration has not been elected or to enforce an arbitration award), jurisdiction and exclusive venue for such litigation shall be in a court located in Los Angeles, California, USA; however, the parties shall also have the right to enforce a judgment of such a court in any court of competent jurisdiction. For the purpose of aiding the arbitration and/or preserving the rights of the parties during the pendency of an arbitration, the parties shall have the right to seek temporary or preliminary injunctive relief from the arbitration panel or in a court located in Los Angeles, California, USA, which shall not be a waiver of this arbitration agreement.

5.9 Limitations on Monetary Remedies for Violations of this Agreement. ICANN's aggregate monetary liability for violations of this Agreement shall not exceed an amount equal to the Accreditation fees paid by Registrar to ICANN under Subsection 3.9 of this Agreement during the preceding twelve-month period. Registrar's monetary liability to ICANN for violations of this Agreement shall be limited to Accreditation fees owing to ICANN under this Agreement and, except in the case of a good faith disagreement concerning the interpretation of this agreement, reasonable payment to ICANN for the reasonable and direct costs including attorney fees, staff time, and other related expenses associated with legitimate efforts to enforce Registrar compliance with this agreement and costs incurred by ICANN to respond to or mitigate the negative consequences of such behavior for Registered Name Holders and the Internet community. In the event of repeated willful material breaches of the agreement, Registrar shall be liable for sanctions of up to five (5) times ICANN's enforcement costs, but otherwise in no event shall either party be liable for special, indirect, incidental, punitive, exemplary, or consequential damages for any violation of this Agreement.

6. AMENDMENT AND WAIVER.

6.1 If the ICANN Board of Directors determines that an amendment to this Agreement (including to the Specifications referred to herein, unless such Specifications expressly do not permit amendment thereto) and all other registrar agreements between ICANN and the Applicable Registrars (the "Applicable Registrar Agreements") is desirable (each, a "Special Amendment"), ICANN may adopt a Special Amendment pursuant to the requirements of and process set forth in this Section 6; provided that a Special Amendment may not be a Restricted Amendment.

6.2 Prior to submitting a Special Amendment for Registrar Approval, ICANN shall first consult in good faith with the Working Group regarding the form and substance of such

Special Amendment. The duration of such consultation shall be reasonably determined by ICANN based on the substance of the Special Amendment. Following such consultation, ICANN may propose the adoption of a Special Amendment by publicly posting such amendment on its website for no less than thirty (30) calendar days (the "Posting Period") and providing notice of such proposed amendment to the Applicable Registrars in accordance with Section 7.6. ICANN will consider the public comments submitted on a Special Amendment during the Posting Period (including comments submitted by the Applicable Registrars).

6.3 If, within one hundred eighty (180) calendar days following the expiration of the Posting Period (the "Approval Period"), the ICANN Board of Directors approves a Special Amendment (which may be in a form different than submitted for public comment, but must address the subject matter of the Special Amendment posted for public comment, as modified to reflect and/or address input from the Working Group and public comments), ICANN shall provide notice of, and submit, such Special Amendment for approval or disapproval by the Applicable Registrars. If, during the sixty (60) calendar day period following the date ICANN provides such notice to the Applicable Registrars, such Special Amendment receives Registrar Approval, such Special Amendment shall be deemed approved (an "Approved Amendment") by the Applicable Registrars, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Approved Amendment to Registrar (the "Amendment Effective Date"). In the event that a Special Amendment does not receive Registrar Approval, the Special Amendment shall be deemed not approved by the Applicable Registrars (a "Rejected Amendment"). A Rejected Amendment will have no effect on the terms and conditions of this Agreement, except as set forth below.

6.4 If the ICANN Board of Directors reasonably determines that a Rejected Amendment falls within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification, the ICANN Board of Directors may adopt a resolution (the date such resolution is adopted is referred to herein as the "Resolution Adoption Date") requesting an Issue Report (as such term is defined in ICANN's Bylaws) by the Generic Names Supporting Organization (the "GNSO") regarding the substance of such Rejected Amendment. The policy development process undertaken by the GNSO pursuant to such requested Issue Report is referred to herein as a "PDP." If such PDP results in a Final Report supported by a GNSO Supermajority (as defined in ICANN's Bylaws) that either (i) recommends adoption of the Rejected Amendment as Consensus Policy or (ii) recommends against adoption of the Rejected Amendment as Consensus Policy, and, in the case of (i) above, the Board adopts such Consensus Policy, Registrar shall comply with its obligations pursuant to Section 4 of this Agreement. In either case, ICANN will abandon the Rejected Amendment and it will have no effect on the terms and conditions of this Agreement. Notwithstanding the foregoing provisions of this Section 6.4, the ICANN Board of Directors shall not be required to initiate a PDP with respect to a Rejected Amendment if, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registrar Approval pursuant to Section 6.3, the subject matter of such Rejected Amendment was the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation.

6.5 If (i) a Rejected Amendment does not fall within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification, (ii) the subject matter of a Rejected Amendment was, at any time in the twelve (12) month period preceding the submission of such Rejected Amendment for Registrar Approval pursuant to Section 6.3, the subject of a concluded or otherwise abandoned or terminated PDP that did not result in a GNSO Supermajority recommendation, or (iii) a PDP does not result in a Final Report supported by a GNSO Supermajority that either (a) recommends adoption of the Rejected Amendment as Consensus Policy or (b) recommends against adoption of the Rejected Amendment as Consensus Policy (or such PDP has otherwise been abandoned or terminated for any reason), then, in any such case, such Rejected Amendment may still be adopted and become effective in the manner described below. In order for the Rejected Amendment to be adopted, the following requirements must be satisfied:

6.5.1 the subject matter of the Rejected Amendment must be within the scope of ICANN's mission and consistent with a balanced application of its core values (as described in ICANN's Bylaws);

6.5.2 the Rejected Amendment must be justified by a Substantial and Compelling Reason in the Public Interest, must be likely to promote such interest, taking into account competing public and private interests that are likely to be affected by the Rejected Amendment, and must be narrowly tailored and no broader than reasonably necessary to address such Substantial and Compelling Reason in the Public Interest;

6.5.3 to the extent the Rejected Amendment prohibits or requires conduct or activities, imposes material costs on the Applicable Registrars, and/or materially reduces public access to domain name services, the Rejected Amendment must be the least restrictive means reasonably available to address the Substantial and Compelling Reason in the Public Interest;

6.5.4 the ICANN Board of Directors must submit the Rejected Amendment, along with a written explanation of the reasoning related to its determination that the Rejected Amendment meets the requirements set out in subclauses (i) through (iii) above, for public comment for a period of no less than thirty (30) calendar days; and

6.5.5 following such public comment period, the ICANN Board of Directors must (i) engage in consultation (or direct ICANN management to engage in consultation) with the Working Group, subject matter experts, members of the GNSO, relevant advisory committees and other interested stakeholders with respect to such Rejected Amendment for a period of no less than sixty (60) calendar days; and (ii) following such consultation, reapprove the Rejected Amendment (which may be in a form different than submitted for Registrar Approval, but must address the subject matter of the Rejected Amendment, as modified to reflect and/or address input from the Working Group and public comments) by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such

matter, taking into account any ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy (a "Board Amendment").

Such Board Amendment shall, subject to Section 6.6, be deemed an Approved Amendment, and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Board Amendment to Registrar (which effective date shall be deemed the Amendment Effective Date hereunder). Notwithstanding the foregoing, a Board Amendment may not amend the registrar fees charged by ICANN hereunder, or amend this Section 6.

6.6 Notwithstanding the provisions of Section 6.5, a Board Amendment shall not be deemed an Approved Amendment if, during the thirty (30) calendar day period following the approval by the ICANN Board of Directors of the Board Amendment, the Working Group, on the behalf of the Applicable Registrars, submits to the ICANN Board of Directors an alternative to the Board Amendment (an "Alternative Amendment") that meets the following requirements:

6.6.1 sets forth the precise text proposed by the Working Group to amend this Agreement in lieu of the Board Amendment;

6.6.2 addresses the Substantial and Compelling Reason in the Public Interest identified by the ICANN Board of Directors as the justification for the Board Amendment; and

6.6.3 compared to the Board Amendment is: (a) more narrowly tailored to address such Substantial and Compelling Reason in the Public Interest, and (b) to the extent the Alternative Amendment prohibits or requires conduct or activities, imposes material costs on Affected Registrars, or materially reduces access to domain name services, is a less restrictive means to address the Substantial and Compelling Reason in the Public Interest.

Any proposed amendment that does not meet the requirements of subclauses 6.6.1 through 6.6.3 in the immediately preceding sentence shall not be considered an Alternative Amendment hereunder and therefore shall not supersede or delay the effectiveness of the Board Amendment. If, following the submission of the Alternative Amendment to the ICANN Board of Directors, the Alternative Amendment receives Registrar Approval, the Alternative Amendment shall supersede the Board Amendment and shall be deemed an Approved Amendment hereunder (and shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice of the approval of such Alternative Amendment to Registrar, which effective date shall deemed the Amendment Effective Date hereunder), unless, within a period of sixty (60) calendar days following the date that the Working Group notifies the ICANN Board of Directors of Registrar Approval of such Alternative Amendment (during which time ICANN shall engage with the Working Group with respect to the Alternative Amendment), the ICANN Board of Directors by the affirmative vote of at least two-thirds of the members of the ICANN Board of Directors eligible to vote on such matter, taking into account any

ICANN policy affecting such eligibility, including ICANN's Conflict of Interest Policy, rejects the Alternative Amendment. If (A) the Alternative Amendment does not receive Registrar Approval within thirty (30) days of submission of such Alternative Amendment to the Applicable Registrars (and the Working Group shall notify ICANN of the date of such submission), or (B) the ICANN Board of Directors rejects the Alternative Amendment by such two-thirds vote, the Board Amendment (and not the Alternative Amendment) shall be effective and deemed an amendment to this Agreement on the date that is sixty (60) calendar days following the date ICANN provided notice to Registrar (which effective date shall deemed the Amendment Effective Date hereunder). If the ICANN Board of Directors rejects an Alternative Amendment, the board shall publish a written rationale setting forth its analysis of the criteria set forth in Sections 6.6.1 through 6.6.3. The ability of the ICANN Board of Directors to reject an Alternative Amendment hereunder does not relieve the Board of the obligation to ensure that any Board Amendment meets the criteria set forth in Section 6.5.1 through 6.5.5.

6.7 In the event that Registrar believes an Approved Amendment does not meet the substantive requirements set out in this Section 6 or has been adopted in contravention of any of the procedural provisions of this Section 6, Registrar may challenge the adoption of such Special Amendment pursuant to the dispute resolution provisions set forth in Section 5.8, except that such arbitration shall be conducted by a three-person arbitration panel. Any such challenge must be brought within sixty (60) calendar days following the date ICANN provided notice to Registrar of the Approved Amendment, and ICANN may consolidate all challenges brought by registrars (including Registrar) into a single proceeding. The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process.

6.8 Registrar may apply in writing to ICANN for an exemption from the Approved Amendment (each such request submitted by Registrar hereunder, an "Exemption Request") during the thirty (30) calendar day period following the date ICANN provided notice to Registrar of such Approved Amendment.

6.8.1 Each Exemption Request will set forth the basis for such request and provide detailed support for an exemption from the Approved Amendment. An Exemption Request may also include a detailed description and support for any alternatives to, or a variation of, the Approved Amendment proposed by such Registrar.

6.8.2 An Exemption Request may only be granted upon a clear and convincing showing by Registrar that compliance with the Approved Amendment conflicts with applicable laws or would have a material adverse effect on the long-term financial condition or results of operations of Registrar. No Exemption Request will be granted if ICANN determines, in its reasonable discretion, that granting such Exemption Request would be materially harmful to registrants or result in the denial of a direct benefit to registrants.

6.8.3 Within ninety (90) calendar days of ICANN's receipt of an Exemption Request, ICANN shall either approve (which approval may be conditioned or consist

of alternatives to or a variation of the Approved Amendment) or deny the Exemption Request in writing, during which time the Approved Amendment will not amend this Agreement.

6.8.4 If the Exemption Request is approved by ICANN, the Approved Amendment will not amend this Agreement; provided, that any conditions, alternatives or variations of the Approved Amendment required by ICANN shall be effective and, to the extent applicable, will amend this Agreement as of the Amendment Effective Date. If such Exemption Request is denied by ICANN, the Approved Amendment will amend this Agreement as of the Amendment Effective Date (or, if such date has passed, such Approved Amendment shall be deemed effective immediately on the date of such denial), provided that Registrar may, within thirty (30) calendar days following receipt of ICANN's determination, appeal ICANN's decision to deny the Exemption Request pursuant to the dispute resolution procedures set forth in Section 5.8.

6.8.5 The Approved Amendment will be deemed not to have amended this Agreement during the pendency of the dispute resolution process. For avoidance of doubt, only Exemption Requests submitted by Registrar that are approved by ICANN pursuant to this Article 6 or through an arbitration decision pursuant to Section 5.8 shall exempt Registrar from any Approved Amendment, and no Exemption Request granted to any other Applicable Registrar (whether by ICANN or through arbitration), shall have any effect under this Agreement or exempt Registrar from any Approved Amendment.

6.9 Except as set forth in Section 4, Subsection 5.3, this Section 6, Section 7.4 and as otherwise set forth in this Agreement and the Specifications hereto, no amendment, supplement or modification of this Agreement or any provision hereof shall be binding unless executed in writing by both parties, and nothing in this Section 6 or Section 7.4 shall restrict ICANN and Registrar from entering into bilateral amendments and modifications to this Agreement negotiated solely between the two parties. No waiver of any provision of this Agreement shall be binding unless evidenced by a writing signed by the party waiving compliance with such provision. No waiver of any of the provisions of this Agreement or failure to enforce any of the provisions hereof shall be deemed or shall constitute a waiver of any other provision hereof, nor shall any such waiver constitute a continuing waiver unless otherwise expressly provided. For the avoidance of doubt, nothing in this Section 6 or Section 7.4 shall be deemed to limit Registrar's obligation to comply with Section 4.

6.10 Notwithstanding anything in this Section 6 to the contrary, (a) if Registrar provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registrar Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registrar, and (b) no Approved Amendment adopted pursuant to Section 6 shall become effective with respect to Registrar if Registrar provides ICANN with an irrevocable notice of termination pursuant to Section 5.4.

7. MISCELLANEOUS PROVISIONS.

7.1 Specific Performance. While this Agreement is in effect, either party may seek specific performance of any provision of this Agreement in the manner provided in Section 5.8, provided the party seeking such performance is not in material breach of its obligations.

7.2 Handling by ICANN of Registrar-Supplied Data. Before receiving any Personal Data from Registrar, ICANN shall specify to Registrar in writing the purposes for and conditions under which ICANN intends to use the Personal Data. ICANN may from time to time provide Registrar with a revised specification of such purposes and conditions, which specification shall become effective no fewer than thirty (30) days after it is provided to Registrar. ICANN shall not use Personal Data provided by Registrar for a purpose or under conditions inconsistent with the specification in effect when the Personal Data was provided. ICANN shall take reasonable steps to avoid uses of the Personal Data by third parties inconsistent with the specification.

7.3 Assignment; Change of Ownership or Management.

7.3.1 Except as set forth in this Section 7.3.1, either party may assign or transfer this Agreement only with the prior written consent of the other party, which shall not be unreasonably withheld. If ICANN fails to expressly provide or withhold its consent to any requested assignment (an "Assignment Request") of this Agreement by Registrar within thirty (30) calendar days of ICANN's receipt of notice of such Assignment Request (or, if ICANN has requested additional information from Registrar in connection with its review of such request, sixty (60) calendar days of the receipt of all requested written information regarding such request) from Registrar, ICANN shall be deemed to have consented to such requested assignment. Notwithstanding the foregoing, (i) ICANN may assign this Agreement without the consent of Registrar upon approval of the ICANN Board of Directors in conjunction with a reorganization, reconstitution or re-incorporation of ICANN upon such assignee's express assumption of the terms and conditions of this Agreement, (ii) Registrar may assign this Agreement without the consent of ICANN to a wholly-owned subsidiary of Registrar upon such subsidiary's express assumption of the terms and conditions of this Agreement, and (iii) ICANN shall be deemed to have consented to an Assignment Request in which the assignee associated with such Assignment Request is a party to a Registrar Accreditation Agreement with ICANN on the terms set forth in this Agreement (provided that such assignee is then in compliance with the terms and conditions of such Registrar Accreditation Agreement in all material respects), unless ICANN provides to Registrar a written objection to such Assignment Request within ten (10) calendar days of ICANN's receipt of notice of such Assignment Request pursuant to this Section 7.3.1.

7.3.2 To the extent that an entity acquires a Controlling interest in Registrar's stock, assets or business, Registrar shall provide ICANN notice within seven (7) days of such an acquisition. Such notification shall include a statement that affirms that

Registrar meets the Specification or Policy on Accreditation criteria then in effect, and is in compliance with its obligations under this Agreement. Within thirty (30) days of such notification, ICANN may request additional information from Registrar establishing compliance with this Agreement, in which case Registrar must supply the requested information within fifteen (15) days. Any disputes concerning Registrar's continued Accreditation shall be resolved pursuant to Section 5.8.

7.4 Negotiation Process.

7.4.1 If either the Chief Executive Officer of ICANN ("CEO") or the Chairperson of the Registrar Stakeholder Group ("Chair") desires to discuss any revision(s) to this Agreement, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed revisions to this Agreement (a "Negotiation Notice"). Notwithstanding the foregoing, neither the CEO nor the Chair may (i) propose revisions to this Agreement that modify any Consensus Policy then existing, (ii) propose revisions to this Agreement pursuant to this Section 7.4 on or before June 30, 2014, or (iii) propose revisions or submit a Negotiation Notice more than once during any twelve month period beginning on July 1, 2014.

7.4.2 Following receipt of the Negotiation Notice by either the CEO or the Chair, ICANN and the Working Group shall consult in good faith negotiations regarding the form and substance of the proposed revisions to this Agreement, which shall be in the form of a proposed amendment to this Agreement (the "Proposed Revisions"), for a period of at least ninety (90) calendar days (unless a resolution is earlier reached) and attempt to reach a mutually acceptable agreement relating to the Proposed Revisions (the "Discussion Period").

7.4.3 If, following the conclusion of the Discussion Period, an agreement is reached on the Proposed Revisions, ICANN shall post the mutually agreed Proposed Revisions on its website for public comment for no less than thirty (30) calendar days (the "Posting Period") and provide notice of such revisions to all Applicable Registrars in accordance with Section 7.6. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registrar Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment by the Applicable Registrars and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days' notice from ICANN to Registrar.

7.4.4 If, following the conclusion of the Discussion Period, an agreement is not reached between ICANN and the Working Group on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (the "Mediation Notice") requiring each party to attempt to resolve the disagreements related to the Proposed Revisions through impartial, facilitative (non-evaluative) mediation in accordance with the terms and conditions set forth below. In the event that a

Mediation Notice is provided, ICANN and the Working Group shall, within fifteen (15) calendar days thereof, simultaneously post the text of their desired version of the Proposed Revisions and a position paper with respect thereto on ICANN's website.

7.4.4.1 The mediation shall be conducted by a single mediator selected by the parties. If the parties cannot agree on a mediator within fifteen (15) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the parties will promptly select a mutually acceptable mediation provider entity, which entity shall, as soon as practicable following such entity's selection, designate a mediator, who is a licensed attorney with general knowledge of contract law and, to the extent necessary to mediate the particular dispute, general knowledge of the domain name system. Any mediator must confirm in writing that he or she is not, and will not become during the term of the mediation, an employee, partner, executive officer, director, or security holder of ICANN or an Applicable Registrar. If such confirmation is not provided by the appointed mediator, then a replacement mediator shall be appointed pursuant to this Section 7.4.4.1.

7.4.4.2 The mediator shall conduct the mediation in accordance with the rules and procedures for facilitative mediation that he or she determines following consultation with the parties. The parties shall discuss the dispute in good faith and attempt, with the mediator's assistance, to reach an amicable resolution of the dispute.

7.4.4.3 Each party shall bear its own costs in the mediation. The parties shall share equally the fees and expenses of the mediator.

7.4.4.4 If an agreement is reached during the mediation, ICANN shall post the mutually agreed Proposed Revisions on its website for the Posting Period and provide notice to all Applicable Registrars in accordance with Section 7.6. ICANN and the Working Group will consider the public comments submitted on the agreed Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars). Following the conclusion of the Posting Period, the Proposed Revisions shall be submitted for Registrar Approval and approval by the ICANN Board of Directors. If such approvals are obtained, the Proposed Revisions shall be deemed an Approved Amendment by the Applicable Registrars and ICANN, and shall be effective and deemed an amendment to this Agreement upon sixty (60) days' notice from ICANN to Registrar.

7.4.4.5 If the parties have not resolved the dispute for any reason by the date that is ninety (90) calendar days following receipt by the CEO or Chair, as applicable, of the Mediation Notice, the mediation shall automatically terminate (unless extended by agreement of the parties). The mediator shall deliver to the parties a definition of the issues that could be considered in

future arbitration, if invoked. Those issues are subject to the limitations set forth in Section 7.4.5.2 below.

7.4.5 If, following mediation, ICANN and the Working Group have not reached an agreement on the Proposed Revisions, either the CEO or the Chair may provide the other person written notice (an "Arbitration Notice") requiring ICANN and the Applicable Registry Operators to resolve the dispute through binding arbitration in accordance with the arbitration provisions of Section 5.8, subject to the requirements and limitations of this Section 7.4.5.

7.4.5.1 If an Arbitration Notice is sent, the mediator's definition of issues, along with the Proposed Revisions (be those from ICANN, Registrars or both) shall be posted for public comment on ICANN's website for a period of no less than thirty (30) calendar days. ICANN and the Working Group will consider the public comments submitted on the Proposed Revisions during the Posting Period (including comments submitted by the Applicable Registrars), and information regarding such comments and consideration shall be provided to a three (3) person arbitrator panel. Each party may modify its Proposed Revisions before and after the Posting Period. The arbitration proceeding may not commence prior to the closing of such public comment period, and ICANN may consolidate all challenges brought by registrars (including Registrar) into a single proceeding. Except as set forth in this Section 7.4.5.1, the arbitration shall be conducted pursuant to Section 5.8.

7.4.5.2 No dispute regarding the Proposed Revisions may be submitted for arbitration to the extent the subject matter of the Proposed Revisions (i) relates to Consensus Policy, (ii) falls within the subject matter categories set forth in Section 1.2 of the Consensus Policies and Temporary Policies Specification , or (iii) seeks to amend any of the following provisions or Specifications of this Agreement: Sections 2, 4 and 6; subsections 3.1, 3.2, 3.3, 3.4, 3.5, 3.7, 3.8, 3.9, 3.14, 3.19, 3.21, 5.1, 5.2 or 5.3; and the Consensus Policies and Temporary Policies Specification, Data Retention Specification, RDDS Accuracy Program Specification, Registration Data Directory Services (RDDS) Specification or the Additional Registrar Operation Specification.

7.4.5.3 The mediator will brief the arbitrator panel regarding ICANN and the Working Group's respective proposals relating to the Proposed Revisions.

7.4.5.4 No amendment to this Agreement relating to the Proposed Revisions may be submitted for arbitration by either the Working Group or ICANN, unless, in the case of the Working Group, the proposed amendment has received Registrar Approval and, in the case of ICANN, the proposed amendment has been approved by the ICANN Board of Directors.

7.4.5.5 In order for the arbitrator panel to approve either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions,

the arbitrator panel must conclude that such proposed amendment is consistent with a balanced application of ICANN's core values (as described in ICANN's Bylaws) and reasonable in light of the balancing of the costs and benefits to the business interests of the Applicable Registrars and ICANN (as applicable), and the public benefit sought to be achieved by the Proposed Revisions as set forth in such amendment. If the arbitrator panel concludes that either ICANN or the Working Group's proposed amendment relating to the Proposed Revisions meets the foregoing standard, such amendment shall be effective and deemed an amendment to this Agreement upon sixty (60) calendar days' notice from ICANN to Registrar and deemed an Approved Amendment hereunder.

7.4.6 With respect to an Approved Amendment relating to an amendment proposed by ICANN, Registrar may apply in writing to ICANN for an exemption from such amendment pursuant to the provisions of Section 6.8.

7.4.7 Notwithstanding anything in this Section 7.4 to the contrary, (a) if Registrar provides evidence to ICANN's reasonable satisfaction that the Approved Amendment would materially increase the cost of providing Registrar Services, then ICANN will allow up to one-hundred eighty (180) calendar days for the Approved Amendment to become effective with respect to Registrar, and (b) no Approved Amendment adopted pursuant to Section 7.4 shall become effective with respect to Registrar if Registrar provides ICANN with an irrevocable notice of termination pursuant to Section 5.4.

7.5 No Third-Party Beneficiaries. This Agreement shall not be construed to create any obligation by either ICANN or Registrar to any non-party to this Agreement, including any Registered Name Holder.

7.6 Notices and Designations. Except as provided in Section 4.4 and Section 6, all notices to be given under this Agreement shall be given in writing at the address of the appropriate party as set forth below, unless that party has given a notice of change of address in writing. Each party shall notify the other party within thirty (30) days of any change to its contact information. Any written notice required by this Agreement shall be deemed to have been properly given when delivered in person, when scheduled for delivery by internationally recognized courier service, or when delivered by electronic means followed by an affirmative confirmation of receipt by the recipient's email server. For any notice of a new Specification or Policy established in accordance with this Agreement, Registrar shall be afforded a reasonable period of time after notice of the establishment of such Specification or Policy is e-mailed to Registrar and posted on the ICANN website in which to comply with that specification, policy or program, taking into account any urgency involved. Notices and designations by ICANN under this Agreement shall be effective when written notice of them is deemed given to Registrar.

If to ICANN, addressed to:

Attention: Registrar Accreditation Notices
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, California 90094-2536 USA
Telephone: +1 310 823-9358

With a required copy to: General Counsel
Email: (As specified from time to time)

If to Registrar, addressed to:

[Registrar Name]
[Courier Address]
[Mailing Address]
Attention: [contact person]
Registrar Website URL: [URL]
Telephone: [telephone number]
e-mail: [e-mail address]

7.7 Dates and Times. All dates and times relevant to this Agreement or its performance shall be computed based on the date and time observed in Los Angeles, California, USA.

7.8 Language. All notices, designations, and Specifications or Policies made under this Agreement shall be in the English language.

7.9 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

7.10 Entire Agreement. Except to the extent (a) expressly provided in a written agreement executed by both parties concurrently herewith or (b) of written assurances provided by Registrar to ICANN in connection with its Accreditation, this Agreement (including the specifications, which form part of it) constitutes the entire agreement of the parties pertaining to the Accreditation of Registrar and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject.

7.11 Severability. If one or more provisions of this Agreement are held to be unenforceable under applicable law, the parties agree to renegotiate such provision in good faith. In the event that the parties cannot reach a mutually agreeable and enforceable replacement for such provision, then (a) such provision shall be excluded from this Agreement; (b) the balance of this Agreement shall be interpreted as if such provision were so excluded; and (c) the balance of this Agreement shall be enforceable in accordance with its terms.

* * * * *

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed in duplicate by their duly authorized representatives.

ICANN	**[Registrar]**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

RDDS ACCURACY PROGRAM SPECIFICATION

Registrar shall implement and comply with the requirements set forth in this Specification, as well as any commercially practical updates to this Specification that are developed by ICANN and the Registrar Stakeholder Group during the Term of the Registrar Accreditation Agreement.

1. Except as provided for in Section 3 below, within fifteen (15) days of (1) the registration of a Registered Name sponsored by Registrar, (2) the transfer of the sponsorship of a Registered Name to Registrar, or (3) any change in the Registered Name Holder with respect to any Registered Name sponsored by Registrar, Registrar will, with respect to RDDS information and the corresponding customer account holder contact information related to such Registered Name:

    a. Validate the presence of data for all fields required under Subsection 3.3.1 of the Agreement in a proper format for the applicable country or territory.

    b. Validate that all email addresses are in the proper format according to RFC 5322 (or its successors).

    c. Validate that telephone numbers are in the proper format according to the ITU-T E.164 notation for international telephone numbers (or its equivalents or successors).

    d. Validate that postal addresses are in a proper format for the applicable country or territory as defined in UPU Postal addressing format templates, the S42 address templates (as they may be updated) or other standard formats.

    e. Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory.

    f. Verify:

        i. the email address of the Registered Name Holder (and, if different, the Account Holder) by sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by Registrar, or

        ii. the telephone number of the Registered Name Holder (and, if different, the Account Holder) by either (A) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by Registrar, or (B) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the Registered Name Holder via web, email or postal mail.

In either case, if Registrar does not receive an affirmative response from the Registered Name Holder, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

2. Except as provided in Section 3 below, within fifteen (15) calendar days after receiving any changes to contact information in RDDS or the corresponding customer account contact information related to any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar will validate and, to the extent required by Section 1, verify the changed fields in the manner specified in Section 1 above. If Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If Registrar does not receive an affirmative response from the Account Holder, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

3. Except as set forth in Section 4 below, Registrar is not required to perform the above validation and verification procedures in Section 1(a) through 1(f) above, if Registrar has already successfully completed the validation and verification procedures on the identical contact information and is not in possession of facts or knowledge of circumstances that suggest that the information is no longer valid.

4. If Registrar has any information suggesting that the contact information specified in Section 1(a) through 1(f) above is incorrect (such as Registrar receiving a bounced email notification or non-delivery notification message in connection with compliance with ICANN's WHOIS Data Reminder Policy or otherwise) for any Registered Name sponsored by Registrar (whether or not Registrar was previously required to perform the validation and verification requirements set forth in this Specification in respect of such Registered Name), Registrar must verify or re-verify, as applicable, the email address(es) as described in Section 1(f) (for example by requiring an affirmative response to a WHOIS Data Reminder Policy notice). If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the Registered Name Holder providing the required verification, Registrar shall either verify the applicable contact information manually or suspend the registration, until such time as Registrar has verified the applicable contact information. If, within fifteen (15) calendar days after receiving any such information, Registrar does not receive an affirmative response from the customer paying for the Registered Name, if applicable, providing the required verification, Registrar shall verify the applicable contact information manually, but is not required to suspend any registration.

5. Upon the occurrence of a Registered Name Holder's willful provision of inaccurate or unreliable contact details as described in Subsection 3.7.7.1 of the Registrar Accreditation Agreement, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration, Registrar shall either terminate or suspend the Registered Name Holder's Registered Name or place such registration on clientHold and clientTransferProhibited, until such time as Registrar has validated the information provided by the Registered Name Holder.

6. The terms and conditions of this Specification shall be reviewed by ICANN in consultation with the Registrar Stakeholder Group on or about the first anniversary of the date that the form of the 2013 Registrar Accreditation Agreement is first executed by a registrar.

7. Nothing within this Specification shall be deemed to require Registrar to perform verification or validation of any customer account holder information where the customer account holder does not have any Registered Names under sponsorship of Registrar.

REGISTRATION DATA DIRECTORY SERVICES (RDDS) SPECIFICATION

1. **Registration Data Directory Services.**

1.1. **Definitions**.

1.1.1. **"Registration Data Access Protocol**" or "**RDAP**" is an Internet protocol that provides "RESTful" web services to retrieve registration metadata from Domain Name Registries and Regional Internet Registries.

1.1.2. "**RDAP Directory Services**" or "**RDAP-RDDS**" refers to a Registration Data Directory Service using the RDAP described in RFC 7481, RFC 7482, RFC 8521, RFC 9082 and RFC 9083, and its successor standards.

1.1.3. "**WHOIS-RDDS**" and "**WHOIS Data Directory Services**" refers to a Registration Data Directory Service using the RDAP described in STD 95 (https://www.rfc-editor.org/refs/ref-std95.txt) , and its successor standards.

1.1.4. "**Registration Data Directory Services**" or "**RDDS**" refers to the collective of WHOIS Data Directory Services and RDAP Directory Services.

1.1.5. "**RDAP Ramp-Up Period**" means the period that ends 3 February 2024.

1.1.6. "**WHOIS Services Sunset Date**" means the date that is 360 days after the expiration of the RDAP Ramp-Up Period, provided that ICANN and the Registrar Stakeholder Group in the RAA may mutually agree to postpone the WHOIS Services Sunset Date. If either the Chief Executive Officer of ICANN ("CEO") or the Chairperson of the Registrar Stakeholder Group ("Chair") desires to discuss postponing the WHOIS Services Sunset Date, the CEO or Chair, as applicable, shall provide written notice to the other person, which shall set forth in reasonable detail the proposed postponement.

1.2. RDAP Directory Services

1.2.1. Registrar shall implement the most recent version of the RDAP Technical Implementation Guide and RDAP Response Profile posted at https://icann.org/gtld-rdap-profile. Registrar will implement new versions of the RDAP Technical Implementation Guide and RDAP Response Profile no later than one hundred eighty (180) calendar days after notification from ICANN.

1.2.2. Registrar shall provide lookup query support for:

1.2.2.1. domain information as described in the section "Domain Path Segment Specification" of RFC 9082; and

1.2.2.2. help information as described in the section "Help Path Segment Specification" of RFC 9082.

1.2.3. ICANN reserves the right to specify alternative formats and protocols approved as "Internet Standards" (as opposed to Informational or Experimental standards) through the applicable IETF processes with respect to registration data. Upon such specification, ICANN shall: (a) work collaboratively with gTLD registries and ICANN-accredited registrars to define all operational requirements necessary to implement the applicable standard; and (b) if applicable, initiate negotiations to define all reporting requirements (if any), and reasonable service level requirements commensurate with similarly situated services.

1.3. WHOIS Data Directory Services

1.3.1. Until the WHOIS Services Sunset Date, Registrar will operate a WHOIS service in accordance with Subsection 3.3.9 of the Registrar Accreditation Agreement.

1.3.2. The format of responses shall follow a semi-free text format outlined below, followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database.

1.3.3. Each data object shall be represented as a set of key/value pairs, with lines beginning with keys, followed by a colon and a space as delimiters, followed by the value.

1.3.4. For fields where more than one value exists, multiple numbered key/value pairs with the same key shall be allowed (for example to list multiple name servers). The first key/value pair after a blank line should be considered the start of a new record, and should be considered as identifying that record, and is used to group data, such as hostnames and IP addresses, or a domain name and registrant information, together.

1.3.5. Subject to the Interim Registration Data Policy for gTLDs as adopted by the ICANN Board in May 2019 and any other applicable Consensus and Temporary Policies, the fields specified in Subsection 1.4 below set forth the minimum output requirements.

1.4. **Domain Name Data:**

1.4.1.1. **Query format:** whois –h whois.example-registrar.tld EXAMPLE.TLD

1.4.1.2. **Response format:**

Additional data elements can be added at the end of the text format outlined below. The data element may, at the option of Registrar, be followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database (provided that any such legal disclaimer must be preceded by such blank line).

Domain Name: EXAMPLE.TLD

Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER[1]
Domain Status: clientDeleteProhibited[2] https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: 5372808-ERL[3]
Registrant Name: EXAMPLE REGISTRANT[4]
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP[5]
Registrant Postal Code: A1A1A1[6]
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234[7]
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Registry Admin ID: 5372809-ERL[8]
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: AA
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 1234
Admin Email: EMAIL@EXAMPLE.TLD
Registry Tech ID: 5372811-ERL[9]
Tech Name: EXAMPLE REGISTRANT TECHNICAL
Tech Organization: EXAMPLE REGISTRANT LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: AA
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLE-REGISTRAR.TLD[10]

---

[1] Data element may be deleted, provided that if the data element is used, it must appear at this location.
[2] Note: all applicable statuses must be displayed in the Whois output.
[3] May be left blank if not available from Registry.
[4] For the Registrant, Admin and Tech contact fields requiring a “Name” or “Organization”, the output must include either the name or organization (or both, if available).
[5] All “State/Province” fields may be left blank if not available.
[6] All “Postal Code” fields may be left blank if not available.
[7] All “Phone Ext”, “Fax” and “Fax Ext” fields may be left blank if not available.
[8] May be left blank if not available from Registry.
[9] May be left blank if not available from Registry.
[10] All associated nameservers must be listed.

Name Server: NS02.EXAMPLE-REGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

1.4.2. The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers (the extension will be provided as a separate field as shown above), email addresses, date and times must conform to the mappings specified in EPP RFCs 5730-5734 so that the display of this information (or values returned in WHOIS responses) can be uniformly processed and understood.

1.5. WHOIS Data Directory Services after the WHOIS Services Sunset Date. If Registrar continues to offer WHOIS Data Directory Services after the WHOIS Services Sunset Date, then Registrar shall comply with the following:

1.5.1. If Registrar continues to offer a WHOIS Data Directory Service available via port 43, Registrar shall do so in accordance with RFC 3912.

1.5.2. Personal Data included in registration data must be redacted in accordance with ICANN Consensus Policies and Temporary Policies;

1.5.3. Registrar must adhere to the requirements related to additional fields of the Consistent Labeling and Display Consensus Policy if they choose to add data fields.

1.5.4. If Registrar provides less registration data in WHOIS Data Directory Services than that available in the RDAP Directory Services, Registrar must add the following disclaimer in the WHOIS Data Directory Services output footer: "The registration data available in this service is limited. Additional data may be available at https://lookup.icann.org."

1.5.5. After the WHOIS Services Sunset Date, in the event of a conflict between the WHOIS Data Directory Service requirements and the requirements of Consensus Policies or any Temporary Policy effective after the WHOIS Services Sunset Date, the Consensus Policies or Temporary Policy shall control, but only with respect to subject matter in conflict.

1.5.6. Until such time that updates are made and effective for Consensus Policies and procedures pursuant to the Phase 1 GNSO Consensus Policy recommendations of the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data, adopted by the ICANN Board in May 2019, as of the WHOIS Services Sunset Date, the following terms in such policies will be interpreted as follows:

1.5.6.1. "WHOIS", "Whois", "Whois service", "Publicly accessible WHOIS", and variations thereof shall be interpreted to refer to RDDS as defined in this Specification.

1.5.6.2. "Whois data", "WHOIS information", "Whois contact information", "Whois query data", "WHOIS output", "Whois entry", and variations thereof shall be interpreted to refer to registration data as referenced in this Specification.

1.6. Cooperation with Transition Studies. If ICANN initiates or commissions a study on the transition of WHOIS Data Directory Services to RDAP Data Directory Services, Registrar shall reasonably cooperate with such study, including by delivering to ICANN or its designee conducting such study, both quantitative and qualitative data related to its experience with its transition from WHOIS Data Directory Services to RDAP Data Directory Services. If the data request is beyond what the Registrar collects in the ordinary course of its operations and beyond the data that Registrar is required to collect and provide to ICANN pursuant to this Agreement, Registrar should voluntarily cooperate to provide the requested information or provide an explanation to ICANN why the Registrar is not able to provide the requested information. The terms of this section do not require Registrar to provide data to ICANN that is beyond what Registrar is obligated to provide ICANN pursuant to other sections of this Agreement. Any data delivered to ICANN or its designee pursuant to this Specification that is appropriately marked as confidential shall be treated as confidential information of Registrar, provided that, if ICANN or its designee aggregates and makes anonymous such data, ICANN or its designee may disclose such data to any third party. Following completion of the transition study for which Registrar has provided data, ICANN will destroy all data provided by Registrar that has not been aggregated and made anonymous.

2. Service Level Agreement for Registration Data Directory Services (RDDS)

2.1. Definitions

2.1.1. **IP address.** Refers to IPv4 or IPv6 addresses without making any distinction between the two. When there is need to make a distinction, IPv4 or IPv6 is used.

2.1.2. **Probes.** Network hosts used to perform tests (see below) that are located at various global locations.

2.1.3. **RTT.** Round-Trip Time or RTT refers to the time measured from the sending of the first bit of the first packet of the sequence of packets needed to make a request until the reception of the last bit of the last packet of the sequence needed to receive the response. If the client does not receive the whole sequence of packets needed to consider the response as received, the request will be considered unanswered.

2.1.4. **SLR.** Service Level Requirement is the level of service expected for a certain parameter being measured in a Service Level Agreement (SLA).

2.2. Service Level Agreement Matrix

2.2.1. Registrar shall meet or exceed each of the following SLRs related to the RDAP-RDDS* services:

	Parameter	SLR (monthly basis)
RDAP-RDDS*	RDAP availability	≤ 864 min of downtime (≈ 98%)
	RDAP query RTT	≤ 4000 ms, for at least 95% of the queries
	RDAP update time	≤ 60 min, for at least 95% of the probes

* These SLRs for RDAP-RDDS are not mandatory until the expiration of the RDAP Ramp-Up Period.

2.2.2. Registrar is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. However, note that there is no provision for planned outages or similar periods of unavailable or slow service; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLR measurement purposes.

2.2.3. Until the WHOIS Services Sunset Date, Registrar shall meet or exceed each of the following SLRs related to the WHOIS Data Directory Services:

	Parameter	SLR (monthly basis)
WHOIS-RDDS	WHOIS-RDDS availability	≤ 864 min of downtime (≈ 98%)
	WHOIS-RDDS query RTT	≤ 4000 ms, for at least 95% of the queries
	WHOIS-RDDS update time	≤ 60 min, for at least 95% of the probes

2.2.4. **RDDS**

2.2.4.1. **RDAP-RDDS**

2.2.4.1.1. **RDAP Availability.** Refers to the ability of the RDAP-RDDS service for Registrar to respond to queries from an Internet user with appropriate data from the relevant registrar system. If 51% or more of the RDAP testing Probes see the RDAP-RDDS service as

unavailable during a given time, the RDAP-RDDS service will be considered unavailable.

2.2.4.1.2. **RDAP-query RTT.** Refers to the RTT of the sequence of packets from the start of an RDAP-RDDS testing probe's TCP connection to its end, including the reception of the HTTPS response for only one HTTPS request. If the RTT is 5 times or more the corresponding SLR/performance specifications, the RTT will be considered undefined.

2.2.4.1.3. **RDAP Update Time.** Refers to the time measured from the receipt of an EPP confirmation to a transform command on a domain name, host or contact, up until at least 51% of the RDAP-RDDS testing Probes detect the changes made.

2.2.4.1.4. **RDAP test**. Means one query sent to a particular IP address of one of the servers of the RDAP-RDDS service. Queries shall be about existing objects in the registrar system and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an RTT 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDAP test are: a number in milliseconds corresponding to the RDAP-query RTT or unanswered.

2.2.4.1.5. **Measuring RDAP parameters**. Every 5 minutes, RDAP-RDDS probes will select one IP address from all the public-DNS registered "IP addresses" of the servers of the RDAP-RDDS service of Registrar being monitored and make an "RDAP test". If an RDAP test result is unanswered, the corresponding RDAP-RDDS service will be considered as unavailable from that Probe until it is time to make a new test.

2.2.4.1.6. **Collating the results from RDAP-RDDS Probes**. The minimum number of verifiably working RDAP-RDDS testing Probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered "inconclusive"; during this situation no fault will be flagged against the SLRs.

2.2.4.1.7. **Placement of RDAP-RDDS Probes**. ICANN will use commercially reasonable efforts to deploy probes for measuring RDAP parameters in data centers with carrier grade connectivity in each of the ICANN geographic regions.

2.2.4.2. **WHOIS-RDDS.** Until the WHOIS Services Sunset Date, Registrar shall comply with the provisions of this Subsection 2.2.4.2.

2.2.4.2.1. **WHOIS-RDDS availability.** Refers to the ability of all the WHOIS-RDDS services for Registrar to respond to queries from an Internet user with appropriate data from the relevant registrar system. If 51% or more of the WHOIS-RDDS testing probes see any of the WHOIS-RDDS services as unavailable during a given time, the WHOIS-RDDS will be considered unavailable.

2.2.4.2.2. **WHOIS query RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the **RTT** is 5-times or more the corresponding SLR, the **RTT** will be considered undefined.

2.2.4.2.3. **Web-based-WHOIS query RTT.** Refers to the **RTT** of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If Registrar implements a multiple-step process to get to the information, only the last step shall be measured. If the **RTT** is 5 times or more the corresponding SLR, the RTT will be considered undefined .

2.2.4.2.4. **WHOIS-RDDS query RTT**. Refers to the collective of "**WHOIS query RTT**" and "**Web-based- WHOIS query RTT**".

2.2.4.2.5. **WHOIS-RDDS update time**. Refers to the time measured from the receipt of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the WHOIS-RDDS services reflect the changes made.

2.2.4.2.6. **WHOIS-RDDS test.** Means one query sent to a particular "**IP address**" of one of the servers of one of the WHOIS-RDDS services. Queries shall be about existing objects in the registrar system and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an **RTT** 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an WHOIS-RDDS test are: a number in milliseconds corresponding to the **RTT** or unanswered.

2.2.4.2.7. **Measuring WHOIS-RDDS parameters.** Every 5 minutes, WHOIS-RDDS probes will select one IP address from all the public-DNS registered "**IP addresses**" of the servers for each WHOIS-RDDS service of Registrar being monitored and make an "WHOIS-**RDDS test**" to each one. If an "WHOIS-**RDDS test**" result is unanswered, the corresponding WHOIS-RDDS service will be considered as unavailable from that probe until it is time to make a new test.

2.2.4.2.8. **Collating the results from WHOIS-RDDS probes.** The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

2.2.4.2.9. **Placement of WHOIS-RDDS probes.** ICANN will use commercially reasonable efforts to deploy probes for measuring WHOIS-RDDS parameters in data centers with carrier grade connectivity in each of the ICANN geographic regions.

2.3. Covenants of Performance Measurement

Registrar shall not interfere with measurement **Probes**, including any form of preferential treatment of the requests for the monitored services. Registrar shall respond to the measurement tests described in this Specification as it would do with any other request from Internet users (for RDDS).

CONSENSUS POLICIES AND TEMPORARY POLICIES SPECIFICATION

1. **Consensus Policies.**

1.1. "***Consensus Policies***" are those policies established (1) pursuant to the procedure set forth in ICANN's Bylaws and due process, and (2) covering those topics listed in Section 1.2 of this document. The Consensus Policy development process and procedure set forth in ICANN's Bylaws may be revised from time to time in accordance with the process set forth therein.

1.2. Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including registrars. Consensus Policies shall relate to one or more of the following:

1.2.1. issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, Registrar Services, Registry Services, or the Domain Name System ("DNS");

1.2.2. functional and performance specifications for the provision of Registrar Services;

1.2.3. registrar policies reasonably necessary to implement Consensus Policies relating to a gTLD registry;

1.2.4. resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names); or

1.2.5. restrictions on cross-ownership of registry operators and registrars or Resellers and regulations and restrictions with respect to registrar and registry operations and the use of registry and registrar data in the event that a registry operator and a registrar or Reseller are affiliated.

1.3. Such categories of issues referred to in Section 1.2 shall include, without limitation:

1.3.1. principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);

1.3.2. prohibitions on warehousing of or speculation in domain names by registries or registrars;

1.3.3. reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property, or (iii) the technical management of the DNS or the Internet (e.g., establishment of reservations of names from registration);

1.3.4. maintenance of and access to accurate and up-to-date information concerning Registered Names and name servers;

1.3.5. procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar, including procedures for allocation of responsibility among continuing registrars of the Registered Names sponsored in a TLD by a registrar losing accreditation; and

1.3.6. the transfer of registration data upon a change in registrar sponsoring one or more Registered Names.

1.4. In addition to the other limitations on Consensus Policies, they shall not:

1.4.1. prescribe or limit the price of Registrar Services;

1.4.2. modify the limitations on Temporary Policies (defined below) or Consensus Policies;

1.4.3. modify the provisions in the Registrar Accreditation Agreement regarding terms or conditions for the renewal, termination or amendment of the Registrar Accreditation Agreement or fees paid by Registrar to ICANN; or

1.4.4. modify ICANN's obligations to not apply standards, policies, procedures or practices arbitrarily, unjustifiably, or inequitably and to not single out Registrar for disparate treatment unless justified by substantial and reasonable cause, and exercise its responsibilities in an open and transparent manner.

2. **Temporary Policies.** Registrar shall comply with and implement all specifications or policies established by the ICANN Board of Directors (the "***Board***") on a temporary basis, if adopted by the Board by a vote of at least two-thirds of its members, so long as the Board reasonably determines that such modifications or amendments are justified and that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the stability or security of Registrar Services, Registry Services or the DNS or the Internet ("***Temporary Policies***").

2.1. Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any Temporary Policy, the Board shall state the period of time for which the Temporary Policy is adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws.

2.1.1. ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the Temporary Policy and why the Board believes such Temporary Policy should receive the consensus support of Internet stakeholders.

2.1.2. If the period of time for which the Temporary Policy is adopted exceeds 90 days, the Board shall reaffirm its temporary adoption every 90 days for a total period not to exceed one year, in order to maintain such Temporary Policy in effect until such time as it becomes a Consensus Policy. If the one year period expires or, if during such one year period, the Temporary Policy does not

become a Consensus Policy and is not reaffirmed by the Board, Registrar shall no longer be required to comply with or implement such Temporary Policy.

3. **Notice and Conflicts.** Registrar shall be afforded a reasonable period of time following notice of the establishment of a Consensus Policy or Temporary Policy in which to comply with such policy or specification, taking into account any urgency involved. In the event of a conflict between Registrar Services and Consensus Policies or any Temporary Policy, the Consensus Polices or Temporary Policy shall control, but only with respect to subject matter in conflict. For the avoidance of doubt, Consensus Policies that meet the requirements of this Specification may supplement or supersede provisions of the agreements between Registrar and ICANN, but only to the extent that such Consensus Policies relate to the matters set forth in Section 1.2 and 1.3 of this Specification.

SPECIFICATION ON PRIVACY AND PROXY REGISTRATIONS

Until the date ICANN implements a Privacy and Proxy Accreditation Program as referenced in Section 3.14 of the Registrar Accreditation Agreement, Registrar agrees to comply, and to require its Affiliates and Resellers to comply, with the terms of this Specification. This Specification may not be modified by ICANN or Registrar.

1. Definitions. For the purposes of this Specification, the following definitions shall apply.

   1.1 "P/P Customer" means, regardless of the terminology used by the P/P Provider, the licensee, customer, beneficial user, beneficiary, or other recipient of Privacy Services and Proxy Services.

   1.2 "Privacy Service" is a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the P/P Provider for display of the Registered Name Holder's contact information in the Registration Data Directory Service (RDDS) or equivalent services.

   1.3 "Proxy Service" is a service through which a Registered Name Holder licenses use of a Registered Name to the P/P Customer in order to provide the P/P Customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Directory Service (RDDS) or equivalent services rather than the P/P Customer's contact information.

   1.4 "P/P Provider" or "Service Provider" is the provider of Privacy/Proxy Services, including Registrar and its Affiliates, as applicable.

2. Obligations of Registrar. For any Proxy Service or Privacy Service offered by Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by Registrar, Registrar and its Affiliates must require all P/P Providers to follow the requirements described in this Specification and to abide by the terms and procedures published pursuant to this Specification.

   2.1 Disclosure of Service Terms. P/P Provider shall publish the terms and conditions of its service (including pricing), on its website and/or Registrar's website.

   2.2 Abuse/Infringement Point of Contact. P/P Provider shall publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights).

   2.3 Disclosure of Identity of P/P Provider. P/P Provider shall publish its business contact information on its website and/or Registrar's website.

2.4 Terms of service and description of procedures. The P/P Provider shall publish on its website and/or Registrar's website a copy of the P/P Provider service agreement and description of P/P Provider's procedures for handling the following:

2.4.1 The process or facilities to report abuse of a domain name registration managed by the P/P Provider;

2.4.2 The process or facilities to report infringement of trademarks or other rights of third parties;

2.4.3 The circumstances under which the P/P Provider will relay communications from third parties to the P/P Customer;

2.4.4 The circumstances under which the P/P Provider will terminate service to the P/P Customer;

2.4.5 The circumstances under which the P/P Provider will reveal and/or publish in the Registration Data Directory Service (RDDS) or equivalent service the P/P Customer's identity and/or contact data; and

2.4.6 A description of the support services offered by P/P Providers to P/P Customers, and how to access these services.

2.5 Escrow of P/P Customer Information. Registrar shall include P/P Customer contact information in its Registration Data Escrow deposits required by Section 3.6 of the Agreement. P/P Customer Information escrowed pursuant to this Section 2.5 of this Specification may only be accessed by ICANN in the event of the termination of the Agreement or in the event Registrar ceases business operations.

3. Exemptions. Registrar is under no obligation to comply with the requirements of this specification if it can be shown that:

3.1 Registered Name Holder employed the services of a P/P Provider that is not provided by Registrar, or any of its Affiliates;

3.2 Registered Name Holder licensed a Registered Name to another party (i.e., is acting as a Proxy Service) without Registrar's knowledge; or

3.3 Registered Name Holder has used P/P Provider contact data without subscribing to the service or accepting the P/P Provider terms and conditions.

DATA RETENTION SPECIFICATION

1. During the Term of this Agreement, for each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain in its own electronic database (as updated from time to time) the data specified below:

   1.1. Registrar shall collect the following information from registrants at the time of registration of a domain name (a "Registration") and shall maintain that information for the duration of Registrar's sponsorship of the Registration and for a period of two additional years thereafter:

      1.1.1. First and last name or full legal name of registrant;

      1.1.2. First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;

      1.1.3. Postal address of registrant, administrative contact, technical contact, and billing contact;

      1.1.4. Email address of registrant, administrative contact, technical contact, and billing contact;

      1.1.5. Telephone contact for registrant, administrative contact, technical contact, and billing contact;

      1.1.6. Data elements in any RDDS service notwithstanding if the data is redacted in the free public available RDDS response;

      1.1.7. Types of domain name services purchased for use in connection with the Registration; and

      1.1.8. To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data.

   1.2. Registrar shall collect the following information and maintain that information for no less than one hundred and eighty (180) days following the relevant interaction:

      1.2.1. Information regarding the means and source of payment reasonably necessary for Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor;

      1.2.2. Log files, billing records and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records containing communications source and destination information, including, depending on the method of

transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the registrant about the Registration; and

1.2.3. Log files and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration.

2. If, based on the receipt of either (i) a written legal opinion from a nationally recognized law firm in the applicable jurisdiction that states that the collection and/or retention of any data element specified herein by Registrar is reasonably likely to violate applicable law (the "Opinion") or (ii) a ruling of, or written guidance from, a governmental body of competent jurisdiction providing that compliance with the data collection and/or retention requirements of this Specification violates applicable law, Registrar determines in good faith that the collection and/or retention of any data element specified in this Specification violates applicable law, Registrar may provide written notice of such determination to ICANN and request a waiver from compliance with specific terms and conditions of this Specification (a "Waiver Request"). Such written notice shall: (i) specify the relevant applicable law, the allegedly offending data collection and retention elements, the manner in which the collection and/or retention of such data violates applicable law, and a reasonable description of such determination and any other facts and circumstances related thereto, (ii) be accompanied by a copy of the Opinion and governmental ruling or guidance, as applicable, and (iii) be accompanied by any documentation received by Registrar from any governmental authority, in each case, related to such determination, and such other documentation reasonably requested by ICANN. Following receipt of such notice, ICANN and Registrar shall discuss the matter in good faith in an effort to reach a mutually acceptable resolution of the matter. Until such time as ICANN's Procedure for Handling Whois Conflicts with Privacy Law is modified to include conflicts relating to the requirements of this Specification and if ICANN agrees with Registrar's determination, ICANN's office of general counsel may temporarily or permanently suspend compliance and enforcement of the affected provisions of this Specification and grant the Waiver Request. Prior to granting any exemption hereunder, ICANN will post its determination on its website for a period of thirty (30) calendar days. Following such modification of ICANN's Procedure for Handling Whois Conflicts with Privacy Law, all Waiver Requests (whether granted or denied) shall be resolved pursuant to such modified procedures.

3. If (i) ICANN has previously waived compliance with the requirements of any requirement of this Data Retention Specification in response to a Waiver Request from a registrar that is located in the same jurisdiction as Registrar and (ii) Registrar is subject to the same applicable law that gave rise to ICANN's agreement to grant such waiver, Registrar may request that ICANN to grant a similar waiver, which request shall

be approved by ICANN, unless ICANN provides Registrar with a reasonable justification for not approving such request, in which case Registrar may thereafter make an Waiver Request pursuant to Section 2 of this Data Retention Specification.

4. Any modification of this Data Retention Specification to address violations of applicable law shall only apply during the period of time that the specific provisions of the applicable law giving rise to such violations remain in effect. If the applicable law is repealed or modified (or preempted) in a manner that would no longer prohibit the collection and/or retention of data and information as originally specified in this Data Retention Specification, Registrar agrees that the original version of this Specification will apply to the maximum extent permitted by such modified applicable law.

REGISTRAR INFORMATION SPECIFICATION

Registrar shall provide to ICANN the information specified below, which shall be maintained in accordance with Section 3.17 of the Agreement. With regard to information identified below, ICANN will hold such information pursuant to the disclosure requirements set forth in Section 3.15 of the Agreement.

General Information

1. Full legal name of Registrar.

2. Legal form of Registrar (e.g., LLC, Corporation, Government Body, Intergovernmental Organization, etc.).

3. The jurisdiction in which Registrar's business is registered for legal and financial purposes.

4. Registrar's business registration number and the name of the authority that issued this number.

5. Every business name and/or trade name used by Registrar.

6. Provide current documentation demonstrating that Registrar entity is legally established and in good standing. For proof of establishment, provide charter documents or other equivalent document (e.g., membership agreement) of the entity. If Registrar is a government body or organization, provide a certified copy of the relevant statute, governmental decision or other instrument under which the government body or organization has been established. With respect to an entity other than a government body or organization, where no such certificates or documents are available in Registrar's jurisdiction, an affidavit drafted and signed by a notary public or a legal practitioner duly qualified in the courts of Registrar's jurisdiction, declaring that the organization is established and in good standing, must be provided.

7. Correspondence address for Registrar.* This address will be used for contractual purposes, and Registrar must be able to accept notices and service of legal process at this address. No Post Office boxes are allowed.

8. Primary phone number where Registrar can be reached for contractual purposes.

9. Primary Fax number where Registrar can be reached for contractual purposes.

10. Primary Email address where Registrar can be reached for contractual purposes.

11. If the location or address of Registrar's principal place of business is different from the address provided in 7, provide details including address, phone number, fax number and email address.* Provide ICANN with current documentation demonstrating that Registrar is legally entitled to do business in the principal place of business.

12. Any other addresses where Registrar will be operated or managed, if different from either its principal place of business or correspondence address provided above. (If so, please explain.) Provide ICANN with current documentation demonstrating that Registrar is legally entitled to do business in each location identified.

13. Primary contact name:

Title
Address
Phone number
Fax number
Email address

14. URL, and Location of Port 43 WHOIS server. After the WHOIS Services Sunset Date, the location of Port 43 WHOIS server is only required to be provided if Registrar continues to offer Whois Data Directory Services.

15. One Registered Name sponsored by Registrar in any gTLD to be used by ICANN in monitoring port 43 WHOIS and RDAP. Regardless of the requirements in Section 3.17 of the Agreement, Registrar shall notify ICANN immediately of any change to this data. A failure to respond with registration data for this Registered Name in port 43 WHOIS and RDAP will be considered a failed RDAP and WHOIS-RDDS test.

Ownership, Directors and Officers Information

16. Full name, contact information, and position of any persons or entities owning at least 5% of the ownership interest in Registrar's current business entity. For each person listed, please specify such person's percentage ownership.

17. Full name, contact information, and position of all directors of Registrar.

18. Full name, contact information, and position of all officers of Registrar.* (Officer names and positions must be publicly displayed.)

19. Full name, contact information, and position of all senior management and other key personnel overseeing the provision of Registrar Services.

20. For every person or entity mentioned in the answers to questions 16 to 19, indicate if that person or entity:

a) within the past ten years, has been convicted of a felony or of a misdemeanor related to financial activities, or has been judged by a court to have committed fraud or breach of fiduciary duty, or has been the subject of a judicial determination that is similar or related to any of these;

b) within the past ten years, has been disciplined by any government or industry regulatory body for conduct involving dishonesty or misuse of funds of others;

c) is currently involved in any judicial or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in items 20(a) or 20(b); or

d) is the subject of a disqualification imposed by ICANN.

Provide details if any of the above events in (a)-(d) have occurred.

21. List all Affiliated Registrars, if any, and briefly describe the Affiliation.

22. For any entities listed in item 21, must provide information required in items 1-14 above.

23. List the ultimate parent entity of Registrar, if applicable.*

Other

24. Does Registrar or any of its Affiliates offer any Privacy Service or Proxy Service (as such terms on defined in the Specification on Privacy and Proxy Registrations)? If yes, list the entities or individuals providing the Privacy Service or Proxy Service.

25. For any entities listed in item 24, provide information required in 1-14 above.

26. Does Registrar utilize or benefit from the services of Resellers?

27. If yes, provide a list of all such Resellers known to Registrar. The information specified in this item 27 shall be made available to ICANN upon request. At such time as ICANN develops a secure method for the receipt and retention of such information, such information shall thereafter be provided to ICANN in accordance with Section 3.17 of the Agreement.

* Items marked with "*" must also be published on Registrar's website.

ADDITIONAL REGISTRAR OPERATION SPECIFICATION

This Specification may be modified by ICANN from time to time after consultation with the Registrar Stakeholder Group (or its successor), provided that such updates are commercially practical with respect to the registrar industry, taken as a whole.

1. DNSSEC

Registrar must allow its customers to use DNSSEC upon request by relaying orders to add, remove or change public key material (e.g., DNSKEY or DS resource records) on behalf of customers to the Registries that support DNSSEC. Such requests shall be accepted and processed in a secure manner and according to industry best practices. Registrars shall accept any public key algorithm and digest type that is supported by the TLD of interest and appears in the registries posted at: https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml and https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xml. All such requests shall be transmitted to registries using the EPP extensions specified in RFC 5910 or its successors.

Registrar must show the DNSSEC-signed status of the domain name in the RDAP Directory Service. Registrar must show the DNSSEC parameters stored in Registrar database in the RDAP Directory Service.

2. IPv6

To the extent that Registrar offers registrants the ability to register nameserver addresses, Registrar must allow both IPv4 addresses and IPv6 addresses to be specified.

3. IDN

If Registrar offers Internationalized Domain Name ("IDN") registrations, all new registrations must comply with RFCs 5890, 5891, 5892, 5893 and their successors. Registrar shall also comply with the IDN Guidelines at https://www.icann.org/en/topics/idn/implementation-guidelines.htm which may be amended, modified, or superseded from time to time. Registrar must use the IDN tables published by the relevant registry.

REGISTRANTS' BENEFITS AND RESPONSIBILITIES SPECIFICATION

Domain Name Registrants' Rights:

1. Your domain name registration and any privacy/proxy services you may use in conjunction with it must be subject to a Registration Agreement with an ICANN Accredited Registrar.
    - You are entitled to review this Registration Agreement at any time, and download a copy for your records.
2. You are entitled to accurate and accessible information about:
    - The identity of your ICANN Accredited Registrar;
    - The identity of any proxy or privacy service provider affiliated with your Registrar;
    - Your Registrar's terms and conditions, including pricing information, applicable to domain name registrations;
    - The terms and conditions, including pricing information, applicable to any privacy services offered by your Registrar;
    - The customer support services offered by your Registrar and the privacy services provider, and how to access them;
    - How to raise concerns and resolve disputes with your Registrar and any privacy services offered by them; and
    - Instructions that explain your Registrar's processes for registering, managing, transferring, renewing, and restoring your domain name registrations, including through any proxy or privacy services made available by your Registrar.
3. You shall not be subject to false advertising or deceptive practices by your Registrar or through any proxy or privacy services made available by your Registrar. This includes deceptive notices, hidden fees, and any practices that are illegal under the consumer protection law of your residence.

Domain Name Registrants' Responsibilities:

1. You must comply with the terms and conditions posted by your Registrar, including applicable policies from your Registrar, the Registry and ICANN.

2. You must review your Registrar's current Registration Agreement, along with any updates.
3. You will assume sole responsibility for the registration and use of your domain name.
4. You must provide accurate information for publication in directories such as the RDAP service, and promptly update this to reflect any changes.
5. You must respond to inquiries from your Registrar within fifteen (15) days, and keep your Registrar account data current. If you choose to have your domain name registration renew automatically, you must also keep your payment information current.

LOGO LICENSE SPECIFICATION

The Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [organization type and jurisdiction] ("Registrar") have entered into a Registrar Accreditation Agreement ("Registrar Accreditation Agreement"), of which this appendix ("Logo License Specification") is a part. Definitions in the Registrar Accreditation Agreement apply in this Logo License Specification.

Registrar wishes to acquire from ICANN, and ICANN wishes to grant to Registrar, a license to use the trademarks listed below the signature block of this Logo License Specification ("Trademarks") in connection with Registrar's role as an ICANN-accredited registrar. Pursuant to and subject to the Registrar Accreditation Agreement, Registrar and ICANN hereby agree as follows:

LICENSE

1. Grant of License. ICANN grants to Registrar a non-exclusive, worldwide right and license to use the Trademarks, during the term of this specification and solely in connection with the provision and marketing of Registrar Services in order to indicate that Registrar is accredited as a registrar of domain names by ICANN. Except as provided in this subsection and Subsection 2.2 of the Registrar Accreditation Agreement, Registrar shall not use the Trademarks, any term, phrase, or design which is confusingly similar to the Trademarks or any portion of the Trademarks in any manner whatsoever.

2. Ownership of Trademarks. Any and all rights in the Trademarks that may be acquired by Registrar shall inure to the benefit of, and are hereby assigned to, ICANN. Registrar shall not assert ownership of the Trademarks or any associated goodwill.

3. No Sublicense. Registrar shall not sublicense any of its rights under this specification to any other person or entity (including any of Registrar's resellers) without the prior written approval of ICANN.

REGISTRATION AND ENFORCEMENT

1. Registration. Registration and any other form of protection for the Trademarks shall only be obtained by ICANN in its name and at its expense.

2. Enforcement. Registrar shall promptly notify ICANN of any actual or suspected infringement of the Trademarks by third parties, including Registrar's resellers or affiliates. ICANN shall have the sole discretion to initiate and maintain any legal proceedings against such third parties; Registrar shall not take any such actions without the prior written approval of ICANN; and ICANN shall retain any and all recoveries from such actions.

3. Further Assurances. Registrar agrees to execute such other documents and to take all such actions as ICANN may request to effect the terms of this specification, including providing such materials (for example URLs and samples of any promotional materials bearing the Trademarks), cooperation, and assistance as may be reasonably required to assist ICANN in obtaining, maintaining, and enforcing trademark registration(s) and any other form of protection for the Trademarks.

TERM AND TERMINATION

This Logo License Specification shall be effective from the date it is signed below by both parties until the Expiration Date, unless this specification or the Registrar Accreditation Agreement is earlier terminated. Each party shall have the right to terminate this specification at any time by giving the other party written notice. Upon expiration or termination of this specification, Registrar shall immediately discontinue all use of the Trademarks.

IN WITNESS WHEREOF, the parties have caused this Logo License Specification to be executed by their duly authorized representatives.

ICANN	[Registrar Name]
By: _____	By: _____
	Name:
	Title:
	Dated: _____

TRADEMARKS:

1. ICANN Accredited Registrar
2.

COMPLIANCE CERTIFICATE

_____, 20__

Pursuant to Section 3.15 of Registrar Accreditation Agreement (the "Agreement"), dated _____, 20__, by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), the undersigned certifies, in his/her capacity as an officer of Registrar and not in his/her individual capacity, on behalf of Registrar as follows:

1. The undersigned is the (must be one of the following: Chief Executive Officer/ President/ Chief Operating Officer/ Chief Financial Officer, or functional equivalent thereof) of Registrar.

2. Registrar has in place processes and procedures intended to establish, maintain, review, test, and modify registrar policies and procedures reasonably designed to achieve compliance with the Agreement.

3. To the best of the undersigned's knowledge and belief, Registrar has performed and complied with all covenants, agreements, obligations and conditions contained in the Agreement that are required to be performed or complied with by it for the calendar year 20___.

The undersigned signs this certificate as of the date indicated under the title.

[REGISTRAR]

By: _____

Name:
Title:

TRANSITION ADDENDUM TO REGISTRAR ACCREDITATION AGREEMENT

This Transition Addendum (this "Addendum") to the Registrar Accreditation Agreement (the "Agreement") by and between the Internet Corporation for Assigned Names and Numbers, a California non-profit, public benefit corporation ("ICANN"), and [Registrar Name], a [Organization type and jurisdiction] ("Registrar"), is dated as of _____, 2013.

WHEREAS, ICANN and Registrar entered into the Agreement as of the date hereof; and

WHEREAS, ICANN acknowledges that implementation by Registrar of certain operational provisions of the Agreement is not possible on the date hereof and will require a reasonable grace period.

NOW THEREFORE, the parties agree as follows:

1. ICANN will not enforce the following provisions and specifications of the Agreement until January 1, 2014: Sections 3.4.1.1, 3.4.1.5, 3.7.10, 3.7.11, 3.12.4, 3.12.7, 3.14, 3.18 and 3.19 of the Agreement; the first sentence of Section 3.7.8 of the Agreement; the WHOIS Accuracy Specification; the Data Retention Specification; and the service level agreements set forth in Section 2.2 of the Registration Data Directory Service (WHOIS) Specification (collectively, the "Transition Provisions").

2. In addition, if immediately prior to the execution of this Addendum Registrar was party to the form registrar accreditation agreement adopted by ICANN in 2009 (the "2009 RAA"), Registrar may use its existing form of registrant registration agreement until January 1, 2014, provided that such agreement complies with Section 3.7.7 of the 2009 RAA.

3. For the calendar year ended December 31, 2013, any certification required pursuant to Section 3.15 shall not require certification as to compliance with the Transition Provisions and may acknowledge the permissible use of the registrant registration agreement under Section 2 hereof.

4. Notwithstanding the foregoing, Registrar agrees to use commercially reasonable efforts to comply with the obligations set forth in the Transition Provisions and transition to a registrant registration agreement that complies with the terms of the Agreement prior to January 1, 2014.

5. Registrar must be fully compliant with the Transition Provisions and Section 3.7.7 of the Agreement as of January 1, 2014, at which date this Addendum shall automatically terminate without action by any party, except as it relates to Section 4 hereof.

6. ICANN and the Registrar Whois Validation Working Group (as defined below) will work together to identify and specify an appropriate set of tools to enable Registrar to complete the across field validation specified in Section 1(e) of the Whois Accuracy Program Specification to the Agreement (the "Across Field Validation"). When such tools are mutually agreed between ICANN and the Registrar Whois Validation Working Group,

ICANN shall provide Registrar written notice of such agreement (which notice shall specify and describe the agreed upon tools). Effective on the one hundred eightieth (180th) calendar day following delivery of such notice by ICANN, Registrar shall comply with the obligations specified in Section 1(e) of the Whois Accuracy Program. Until such time, ICANN will not enforce compliance with such obligations.

For purposes of this Section 6, the Registrar Whois Validation Working Group shall be deemed to have agreed to such Across Field Validation tools when Approval (as defined below) of the then serving members of the group is obtained through a vote of the group (which vote may be conducted through any verifiable means determined by the group, including through electronic means).

The "Registrar Whois Validation Working Group" means that existing working group whose membership has been tasked with identifying and specifying a set of tools to enable registrars to complete the Across Field Validation. The membership of the Registrar Whois Validation Working Group shall be made up of volunteering representatives of ICANN-accredited registrars, and shall initially consist of the members currently serving on the existing working group.

"Approval" is obtained following a vote of the Registrar Whois Validation Working Group, if the votes cast in favor of adoption of the proposed Across Field Validations tools by the then serving members of the group are at least two-thirds of the votes cast by such members, with abstentions or non-votes not being counted as either votes in favor or against adoption of such tools. For purposes of the vote of the group as referenced above, (i) only persons appointed by an ICANN-accredited registrar shall be deemed members of the group and eligible to cast a vote as described above and (ii) no ICANN-accredited registrar nor group of Affiliated Registrars represented in the Registrar Whois Validation Working Group shall have more than one vote.

7. Except as set forth in this Addendum, the Agreement shall be in full force and effect, enforceable by the parties in accordance with its terms.

[signature page follows]

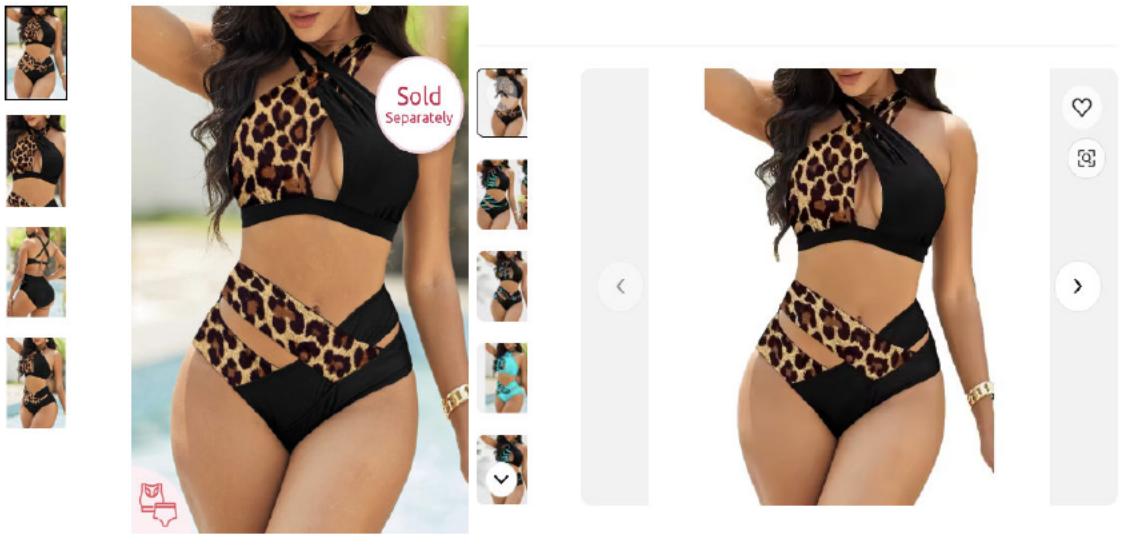
IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be executed in duplicate by their duly authorized representatives.

ICANN	**[Registrar]**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

Exhibit 5

Hong Kong Leyuzhen Technology Co. Limited v. Shenzhen Yilanya Technology Co. Ltd.
Infringement Evidence Copyright VA0002379894

Rotita Copyright Image **Defendant Infringing Image**



https://www.alibaba.com/product-detail/Summer-Plus-Size-5XL-Sexy-Leopard_1601048952193.html?spm=a2700.picsearch.normal_offer.d_image.4f6e5f938NuMOY

Product details

Sold by: **Shenzhen Yilanya Technology Co., Ltd.** Chat now

Product name	Spec/Specs	Unit price	Quantity	Total
Summer Plus Size 5XL Sexy Leopard Two Piece Women Swimsuits Bikini Set Swimwear Beachwear	Color: 1,Size: XXL	USD 6.9600 /Sets ~~USD 6.7000 /Sets~~	1.00	USD 6.96 ~~USD 6.70~~

Product Quantity: **1.00** Total Price: **USD 6.96**

Shipment details

Waiting for supplier to ship Track shipment(s)

Shipping address
Jane Anderson, [redacted]
Street,Chicago,Illinois,United States of America,60613
Modify shipping address

Ship from
CN

Shipping method
Multimodal transport
Ocean+Express US(Economy)
Alibaba.com Logistics

Incoterms and duties
DDP

Summer Plus Size 5XL Sexy Leopard Two Piece Women Swimsuits Set Swimwear Beachwear

No reviews yet

Shenzhen Yilanya Technology Co., L5 yrs · CN

Customizable

20% off

$6.96 / set 1 set(MOQ)

~~$8.70~~

Import charges included

Sample price $8.70 Get sampl

Variations

Select no

Color(4): 1

Size(8)

Shipping

Import charges included in shipping fee

Parcel for General Goods US(Change

Shipping fee $10.63 for 1 set

Estimated delivery by Jul 14-Jul 21

Start orde Add to car Chat nov

$5 off $199

Dropship this product to your store

Start dropshipping

4 interest-free payments with

Afterpay PayPal Klarna

Protections for this product

Secure payments

Every payment you make on Aliba secured with strict SSL encryption and PC DSS data protection protocols

Supplier highlights: This manufacturer and trader mainly exports to the United States, Aust ralia, and the UAE, with a ... and ...

Other recommendations for your business

All 5 colors

Iron Chain Sexy Bikinis Se Two Piece Swimming Suit

$5.56

~~$6.95~~ 20% off

Min. order: 1 set

Easy Return

All 5 colors

Wholesale 6colors S-L Custom Design Pattern...

$6.30

~~$7.87~~ 20% off

Min. order: 1 set

Easy Return

All 3 colors

New Design Crystal Diamond Women Custom

$9.68

~~$12.10~~ 20% off

Min. order: 1 set

Easy Return

Wom Bana

$9.

~~$12.~~

Min.

Easy

Attributes | Performance | Reviews | Supplier | Description

Key attributes

Industry-specific attributes

Material	100% Polyester
Style	Cover Up

Other attributes

Neckline	Round Neck
Gender	Women
Pattern Type	Floral

Show more

Lead time

Customization options

Customized logo (Min. order: 500 sets)
Customized packaging (Min. order: 100 sets)
Graphic customization (Min. order: 500 sets)

Chat now

Ratings & Reviews

Product reviews (0) | Storereviews (235)

No product reviews yet

Go to Store reviews to see reviews for other products

Know your supplier

Erandear

Shenzhen Yilanya Technology Co., Ltd.

Manufacturer, Trading Company, Agent, Others | 5 yrs on Alibaba.com

Located in CN

Online store performance

Easy Return & Refund

Claim a refund if your order is missing o
arrives with product issues, plus free lo
returns for defects on qualifying purcha

Alibaba.com protects all your orders placed and on the platform wit Trade Assurance

On-time delivery rate	Online revenu	Response Time
100.0%	US$ 5,000+	≤4h

More products | Company profile

Product descriptions from the supplier

Specification

Material	nylon
Season	Summer
Size	S/M/L/XL/2XL/3XL/4XL/5XL
MOQ	1SET
Fabric	Polyester
Packing	opp bag+carton or customize size
Sleeve	Swimwear,Two Piece Swimsuit Bikini Set Swimw Swimsuits
OEM	available
Gender	women

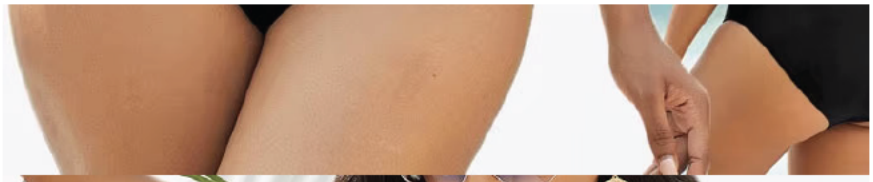
Size/尺码	BUST/胸部	WAIST/腰部	HIP/臀部
S	78-82cm	66-80cm	80-84cm
M	82-86cm	80-84cm	84-88cm
L	86-90cm	84-88cm	88-92cm
XL	90-94cm	88-92cm	92-96cm
2XL	94-98cm	92-96cm	96-100cm
3XL	98-102cm	96-100cm	110-104c
4XL	102-106cm	110-104cm	104-108c
5XL	106-110cm	104-108cm	108-112c
6XL	110cm-114cm	108-112cm	112-116c

Please allow 1-2cm deviations due measurement. Thanks for your unders

由于手动测量，请允许1-2厘米的偏差。 感

Product Description

Welcome to message us online to get all desig
picture!



Recommended by seller

Summer Triangle Brazi	Womans Three 3 Piece	Custom 3D Flower Pus	Wholesale
$6.40/ set	**$9.84**/ set	**$7.20**/ set	**$6.30**/ set
1 set	1 set	1 set	1 set

New Arrival Long Sleev	Summer Beachwear C	Custom Private Label C	Custom Re
$5.90/ set	**$9.24**/ set	**$5.60**/ set	**$6.24**/ set
1 set	1 set	1 set	1 set

New Design Crystal Di	New Women Printed S.	2024 Women Swimwea
$9.68/ set	$7.20-13.28/ set	$7.12/ set
1 set	1 set	1 set

Custom Service

CUSTOMIZE LOGO 1

CUSTOMIZE LOGO 2

CUSTOMIZE LOGO

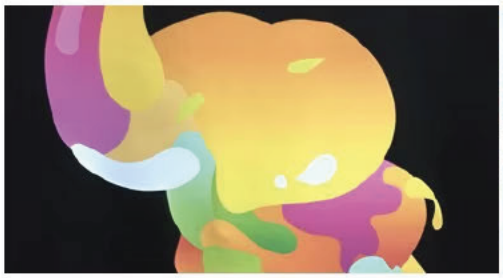
.

CUSTOMIZE DETAILS AS YOU LIKE

- Printing Process -

Screen printing
-
MOQ 10Pcs

EMBROIDERY
-
MOQ 10Pcs



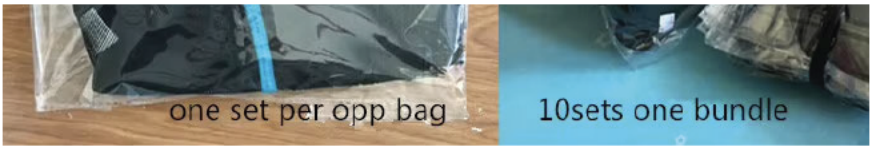
DIGITAL HOT STAMPING
-
MOQ 10Pcs

Automatic pyrogr
-
MOQ 50Pcs

DIGITAL DIRECT INJECTION
-
MOQ 1Pc

Gold Stamping
-
MOQ 10Pcs

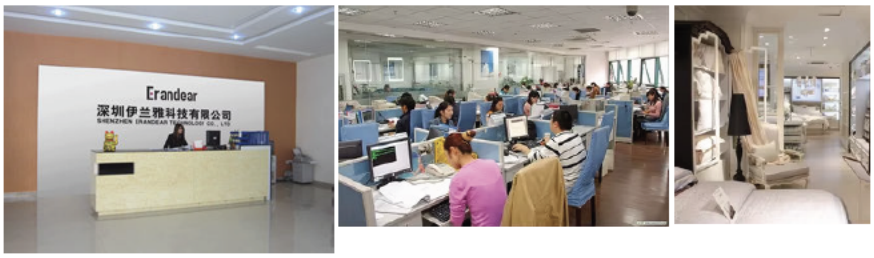
Packing & Delivery



PACKING&SHIPPING

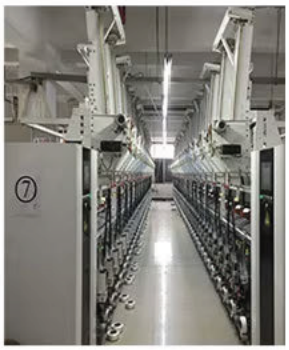
each set In Poly bags ,then 50pcs in woven bag or carton,or customized
short sleeve kids sleep,sleepwear for children,cheap kids pajamas

Company Profile



PRODUCTION PROCESS

equipment

Erandear Company own 10 years home textile series products OEM , ODM and export people own more than 6 years home use sale experience at least. this can make us bus much easily and safety each other.
As our factory is located in the largest home textile market in China, we can get all the information, such as the latest fabric, newdesigns and the best prices. We can provide designs each year to meet different clients' needs.

FAQ

delivery time ?
A: Generally it is 1 - 3 days if the goods are in stock. 10 - 15 days for customize Order , factory Order
quantity.
Q: Do you provide samples ? is it free or extra ? A: Yes , offer the sample not free.we pa cost in
sample , we believe our product can bring more selling status for you , double sample f refund in bulk orders ,
it show the sincere for you for us.
Q: What is your terms of payment ? A: TT , West union . in Bulk Order , 30% Deposit Firs Balance (70%) Before Shipping.
Q: Do you accept customize ? A: Yes , customize order is highly welcome , we respect customer 's ideas and designs .

Contact

Frequently bought together

All 13 colors
2021 Women Plus Size Outfit shirt Pants Set 2 Piece Sport
$4.40-5.76
~~$5.50-7.20~~20% off
Min. order: 1 set
Easy Return

All 11 colors
Ice Silk Thongs for Women Panties High Quality Female.
$2.34
~~$2.93~~20% off
Min. order: 1 set
Easy Return

Christmas Moose Family Matching Clothes Pajamas S
$4.80-7.10
~~$6-8.88~~20% off
Min. order: 2 sets
Easy Return

All 4 colors
Lace 5pcs Soft Silk Women Pajamas Sets Suspenders...
$12-14.10
Min. order: 1 set
Easy Return

All 2 colo
New Arrivals Su Sleepwear Two
$8.84
~~$11.05~~20% off
Min. order: 2 se
Easy Return

Supplier's popular products

Alibaba Guaranteed
Stock Factory Sexy Sunscreen Casual Style...
$6.60
~~$8.25~~20% off
Min. order: 1 piece
Delivery by Jul 14
Money-back guarantee

All 25 colors
US America Custom Desig Sexy Women Basketball...
$8.16
~~$10.20~~20% off
Min. order: 1 set
Easy Return

All 7 colors
King Mcgreen Star 3PCS Sexy Mesh Sheer Strappy
$6.32
~~$7.90~~20% off
Min. order: 1 set
Easy Return

New Arrival Summer Bodysuits for Women Ruff
$6.80
~~$8.50~~20% off
Min. order: 3 sets
Easy Return

Pure Cotton Female Cotto Linen Pleated Short Sleev
$8.52
~~$10.65~~20% off
Min. order: 60 sets
Easy Return

All 4 colors
2022 New Arrivals Summe Crop Top Two Piece Shor
$8.33
Min. order: 1 piece
Easy Return

All 2 colors
Custom Printing Girls Swimwear Beachwear Hig
$6.80
~~$8.50~~20% off
Min. order: 3 sets
Easy Return

All 18 colors
2022 New Designer Bikini Woman Glitter Halter Nec
$6.94
~~$7.71~~10% off
Min. order: 1 set
Easy Return

Whole Living Room Carpe Anti Slip Bedroom Carpet.
$2.50-12.90
Min. order: 1 square meter
Easy Return

3-6 Days Fast Shipping in Stock Brand Name...
$6.66
~~$8.33~~20% off
Min. order: 5 sets
Easy Return

2025 Swimwear Women Luxury Bathing Suits...

$6.66

Min. order: 2 sets

Easy Return

All 7 colors

Plus Size S-3XL Camo Shorts Skirt Pants Women

$7-9.70

Min. order: 2 sets

Easy Return

All 4 colors

Women Beach Transparer Mesh Sarong Soft Gauze..

$2.80-5.56

~~$3.50-6.95~~ 20% off

Min. order: 10 pieces

Easy Return

All 3 colors

Summer Plain Color Swimming Suit Designer...

$5.23

~~$5.88~~ 11% off

Min. order: 2 sets

Easy Return

All 11 colors

Open Back Multi Color Sp Bikini Three Piece Swimw

$5.04

~~$5.66~~ 11% off

Min. order: 2 sets

Easy Return

All 7 colors

Summer Custom 3 Piece Designer Matching...

$7.26

~~$10.08~~ 32% off

Min. order: 1 set

Easy Return

Wholesale Custom Childre Bikini Toddler Swimsuit Gi

$8.80

~~$11~~ 20% off

Min. order: 10 sets

Easy Return

All 2 colors

Hot Sale S to 4XPlus Size Women Swimsuits Summe

$7.92

~~$9.90~~ 20% off

Min. order: 1 set

Easy Return

All 5 colors

2024 V Neck Boxers Brazilian Bikinis Printed...

$5.78

~~$7.23~~ 20% off

Min. order: 2 sets

Easy Return

All 14 colors

Wholesale Sexy Bikinis Atacados Woman Women

$6.80

~~$8.50~~ 20% off

Min. order: 1 set

Easy Return

All 13 colors

2024 New Trend Underwi Bralette Girls Swimwear...

$5.72

~~$7.15~~ 20% off

Min. order: 1 set

Easy Return

All 9 colors

Custom Swimsuit Sport Bathing Suit Boyleg Two...

$5.58

~~$6.97~~ 20% off

Min. order: 2 sets

Easy Return

All 8 colors

Fashion Show Swimwear Women Sexy Two Piece...

$7.04

~~$8.80~~ 20% off

Min. order: 1 set

Easy Return

All 7 colors

2025 Factory Direct Sales Comfortable Sexy Europe

$5.80

~~$7.25~~ 20% off

Min. order: 3 sets

Easy Return

All 6 colors

Swimwear Women Luxury Bathing Suits Woman...

$6.80

~~$8.50~~ 20% off

Min. order: 1 set

Easy Return

All 7 colors

Alibaba Guaranteed

2025 New Arrivals Cute Wholesale Bikini Set Plain

All 5 colors

2025 New Fashion Girl Swimwear Designer...

$5.59

All 5 colors

New

2025 Newest Swimwear Women Luxury Bathing Su

All 5 colors

New

New Arrivals Sexy 2 Piece Women Swimwear De La..

Alibaba Guaranteed

Women Fashion New De Lace One Piece Swim Sui

$6

$5.59
~~$6.99~~20% off
Min. order: 2 sets
Delivery by Jul 14

~~$6.99~~20% off
Min. order: 2 sets
Easy Return

$5.60
~~$7~~ 20% off
Min. order: 2 sets
Easy Return

$5.60
~~$7~~ 20% off
Min. order: 2 sets
Easy Return

~~$7.50~~20% off
Min. order: 1 piece
Delivery by Jul 14
Money-back guarantee

All 5 colors
Custom One Piece Bodysı Swim Suit Womens…
$6.60
~~$8.25~~20% off
Min. order: 3 sets
Easy Return

All 5 colors
2025 Women Bathing Suit Swimwear Sexy Fashion V
$6.60
~~$8.25~~20% off
Min. order: 3 sets
Easy Return

All 5 colors
Female Sexy Solid Beach Backless Swimsuit…
$6.60
~~$8.25~~20% off
Min. order: 3 sets
Easy Return

All 6 colors
Summer New Women's Se Mesh Swimwear Bath Suit
$7.78
~~$9.73~~20% off
Min. order: 3 sets
Easy Return

All 5 colors
2025 Custom Private Labı Bikini High Quality Sexy G
$5.59
~~$6.99~~20% off
Min. order: 2 sets
Easy Return

Related searches

kids swimwear | modest swimwear | boys swimwear | cheap swimwear | arena swimwear | mens swimwear | retro swimwear | skimpy swimwear | sheer swimwear | frozen swimwear | girls swimwear | venus swimwear | thong swimwear | baby swimwear | xoxo swimwear

Report abuse

Erandear

SHENZHEN ERANDEAR TECHNOLOGY CO., LTD

5YRS Shenzhen Yilanya Technology Co., Ltd.

COMPANY OVERVIEW

Company Album 3

Basic Information

Erandear Company own 10 years home textile series products OEM , ODM and export experience. and our sales people own more than 6 years home use sale experience at least. this can make us business comminication much easily and safety each other. As our factory is located in the largest home textile market in China, we can get all the latest fabric designs and information, such as the latest

4.7/5
Satisfied
50 Reviews

Supplier Index	
Transactions	-
Response Time	≤4h
Response rate	92.55

Business type	Manufacturer, Trading Company, Agent, Other	Country / Region	Guangdong, China
Main Products	Apparel, women's sleepwear, women's clothing, women's set, carpet	Total employees	5 - 10 People
Total Annual Revenue	US$50 Million - US$100 Million	Year established	2021
Certifications	-	Product Certifications	-
Patents	-	Trademarks	-
Main Markets	Western Europe 20.00% North America 18.00% Eastern Europe 10.00%		

Selected products

Modern Minimalist Wave Pattern Tufted Flocked...

Modern Non-Slip Absorbent Foot Mat...

Modern Customize Bathroom Foot Mat Non-...

High Quality 3D Functional Simple

PRODUCT CAPACITY

Contact Supplier

Chat Now!

Factory Information

Factory Size	10,000-30,000 square meters
Factory Country/Region	No.26, Group 12, Hongzhong Village, Dongtai Town, Dongtai City, Jiangsu Province, China
No. of Production Lines	6
Contract Manufacturing	OEM Service Offered, Design Service Offered, Buyer Label Offered
Annual Output Value	US$50 Million - US$100 Million

R&D CAPACITY

Research & Development

5 - 10 People

TRADE CAPABILITIES

Main Markets & Product(s)

Main markets	Total Revenue(%)	Main Product(s)	Ver
Western Europe	20.00%	-	-
North America	18.00%	-	-
Eastern Europe	10.00%	-	-
Northern Europe	9.00%	-	-
Southern Europe	8.00%	-	-
Southeast Asia	8.00%	-	-
Mid East	5.00%	-	-
Central America	5.00%	-	-
South America	5.00%	-	-
Eastern Asia	4.00%	-	-

South Asia	3.00%	-	-
Africa	2.00%	-	-

View More Trade Capabilities

Buyer Interaction

Response rate	Response time	Quotation Performance
92.55%	≤4h	24

Transaction History

Transactions	Total Amount
-	-

Contact Supplier

Chat Now!

Send message to supplier

To: Rose Lai

* Message: Enter your inquiry details such as product name, color, size, quantity, material, etc.

0/8000

Send

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

HONG KONG LEYUZHEN TECHNOLOGY CO. LIMITED, Plaintiff, v. Shenzhen Yilanya Technology Co., Ltd., Defendants.	**Case No.: 1:25-cv-04947-MMP-HKM** **Honorable Martha M. Pacold** **Magistrate Heather K. McShain**

DECLARATION OF LIANGJIE LI IN SUPPORT OF PLAINTIFF'S RENEWED MOTION FOR TEMPORARY RESTRAINING ORDER

I, Liangjie Li, of Hong Kong, a special administrative region of the People's Republic of China, declare and state as follows:

1. This declaration is based upon my personal knowledge of the facts stated herein. If called as a witness, I could and would testify as to the statements made herein.

2. I make this declaration in support of Plaintiff's Renewed Motion for Temporary Restraining Order (the "Motion")

3. I am the Chief Operations Officer for Plaintiff Hong Kong Leyuzhen Technology Co. Ltd. ("Plaintiff"). I make this declaration from my matters within my own personal knowledge unless stated otherwise.

4. Plaintiff markets and sells women's clothing and related items under the "Rotita" brand name ("Rotita").

5. Plaintiff is the owner of U.S. Copyright Number VA0002379894, that was duly and legally issued by the United States Copyright Office (the "Copyright Protected Images"), which is attached to the First Amended Complaint as Exhibit 1 (Dkt. No. 22-1).

6. Plaintiff has registered a number of its images and designs with the United States Copyright Office.

7. Plaintiff designs, manufactures, sells, and distributes a wide variety of products including Women's clothing and apparel (collectively, "Plaintiff's Products").

8. Plaintiff generates approximately $20,000,000 in revenue, and well over $1,000,000 derived from sales from the State of Illinois, from sales of its products through its website, rotita.com and does not sell or offer or authorize the sale of its merchandise on any other online platform, such as Amazon, eBay®, Aliexpress, Alibaba, Walmart, or TikTok, and several other online and offline stores.

9. The women's clothing and apparel claimed in the Asserted Copyright Registration have been highly commercially successful.

10. Plaintiff incorporates a variety of copyright-protected original works of authorship in its products.

11. Plaintiff has not granted any licenses of rights to Defendant under the Copyright Protected Images. The Defendant is not an authorized retailer of genuine versions of Plaintiff's Products.

12. Plaintiff is the lawful assignee of all right, title, and interest in the Asserted Copyright.

13. Plaintiff uses its Copyright Protected Images extensively in connection with the marketing of Plaintiff's Products. Plaintiff has expended significant sums in advertising, promoting, and marketing Plaintiff's Products featuring Plaintiff's Copyright Protected Images.

14. Plaintiff's Products embody the same photographs in the Copyrighted Protected Images and registrations. Plaintiff uses its Copyright Protected Images extensively in connection with the marketing of its photographed Products.

15. Plaintiff uses its Copyright Protected Images extensively in connection with the marketing of its Products for planned collection releases throughout each year. The women's clothing and apparel claimed in the Asserted Copyright Registration have been highly commercially successful, bringing in substantial revenue, with new images and photographs being released on a rolling cycle to keep up with changing fashion trends.

16. The products of the women's clothing and apparel embodying the Asserted Copyrights differentiate such women's clothing and apparel from those of competitors.

17. The marketplace success of Plaintiff's Products has resulted in significant copying and counterfeiting of such products. I have, therefore, instituted a worldwide anti-counterfeiting program and regularly investigates suspicious e-commerce stores identified in proactive internet sweeps and reported by consumers.

18. Plaintiff has identified numerous fully interactive e-commerce stores, including those operating the Defendant Internet Stores, which were offering for sale and/or selling Defendant's Infringing Products to consumers in this Judicial District and throughout the United States. ***See*** **Exhibit 5** to the Declaration of Katherine Kuhn ("Kuhn Decl.") (screen-captures showing Defendant's use of the Copyright Protected images to sell competing products and the associated Alibaba stores).

19. All Defendants' online stores located on the Platform utilize the reputation of Plaintiff's Rotita brand to market and sell inferior, competing products by displaying Plaintiff's Copyright protected product images after they are first displayed on the company's website as part of Rotita's yearly product launches for its swimwear Collections. To keep up with fashion trends and seasons each year, Rotita will publish various photos and images to advertise its collections of women's clothing to sell, including the Copyrighted works at issue in this action from the swimwear collection.

20. Defendant's unauthorized use of Plaintiff's copyright registration has caused, and continues to cause, irreparable harm to Plaintiff through loss of exclusivity and loss of future revenue.

21. Given the nature of the fashion industry and my first-hand knowledge of Plaintiff's operations, such large-scale sales operations over online retail platforms require considerable supply chain coordination efforts that could not reasonably be accomplished independently by the Defendant.

22. Since 2009, Plaintiff has invested substantial time, money, and effort advertising the copyrighted photographs claimed in its Copyright registrations.

23. Defendant's unauthorized use of the Copyright Protected Images has and continues to irreparably harm Plaintiff through diminished goodwill and brand confidence, damage to Plaintiff's reputations, loss of exclusivity, and loss of future sales.

24. The extent of the harm to Plaintiff's reputation, the goodwill associated therewith, and the possible diversion of customers due to loss in brand confidence are irreparable and incalculable, thus warranting an immediate halt to Defendant's infringing activities through injunctive relief.

25. Plaintiff will suffer immediate and irreparable injury, loss, or damage if an *ex parte* Temporary Restraining Order is not issued in accordance with Federal Rule of Civil Procedure 65(b)(1).

26. Defendant has been profiting and continues to profit from the sale of Infringing Products.

27. Defendant has eliminated the exclusivity that Plaintiff was entitled to under the Copyright Act.

I declare under penalty of perjury under the law of the United States of America that the foregoing is true and correct.

Executed on July 3, 2025, in Hong Kong

By: */s/ Liangjie Li*_____
LIANGJIE LI

CERTIFICATE OF SERVICE

I hereby certify that on the 3rd day of July 2025, I electronically filed the foregoing document with the clerk of the court for the U.S. District Court, Northern District of Illinois, Eastern Division, using the electronic case filing system. The electronic case filing system sent a "Notice of Electronic Filing" to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

By: */s/ Katherine M. Kuhn*
Katherine M. Kuhn (Bar No. 6331405)
BAYRAMOGLU LAW OFFICES LLC
233 S. Wacker Drive, 44th Floor, #57
Chicago, IL 60606
Tel: (702) 462-5973 Fax: (702) 553-3404
Katherine@bayramoglu-legal.com
Attorneys for Plaintiff