Exhibit 2



2015 Out-of-Cycle Review of Notorious Markets

★ ★ ★

OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

DECEMBER 2015

Emerging Marketing and Distribution Tactics in Internet-Facilitated Counterfeiting

This year, USTR is highlighting emerging trends in the marketing and distribution of counterfeit goods online. The Internet provides many new opportunities for economic growth, encouraging innovation, and the development of new business models. The Internet can also be used to carry out infringing activity due to the ease of conducting commerce through unverified vendors, inability for consumers to inspect goods prior to purchase, and deceptive marketing. In this OCR and in recent years, rights holders have noted escalating levels of counterfeit sales online and an increase in the services that support such operations. With an estimated fifteen percent increase in online sales of counterfeit goods last year, the economic toll of counterfeiting on governments, businesses, and consumers is mounting.[14] Internet-facilitated counterfeiting includes e-commerce sites that provide large-scale platforms for counterfeit sellers and wholesalers to reach a global consumer base such as auction sites, business-to-business (B2B, also known as trade boards), consumer-to-consumer (C2C), and business-to-consumer (B2C) sites. It also includes individual, one-off websites offering counterfeit versions of branded products or mimicking the look and feel of a legitimate retailer.

In the case of standalone websites, there can be tens of thousands of websites targeting a single brand making it difficult to identify a notorious example when these online one-off markets have lower popularity. The List therefore cannot capture the scope and scale of this global problem. These illicit sites use deceptive tactics including cybersquatting (such as nominated sites HTTP://MACYS-SHOES.COM and MACYSKOREA.COM), typosquatting (for example, MACIYS.COM, MAXCYS.COM, and MWCYS.COM) and search engine optimization manipulation to hijack genuine traffic and lure customers to counterfeit offerings.[15] Increasingly sophisticated criminals operate networks of hundreds of sites, use paid search ads and social media campaigns to promote their illegitimate sites, and use mobile apps to solicit sales.

[14] For a discussion of the costs of counterfeiting, including online counterfeiting see Net Names, "Counting the Cost of Counterfeiting," Oct. 2015, available at http://www.netnames.com/blog/wp-content/uploads/2015/10/NetNames-Counterfeiting-Report-A4-2015.pdf

[15] Brand enforcement company MarkMonitor saw a 22 percent increase in cybersquatting in 2014 (https://www.markmonitor.com/download/Infographics/MarkMonitor.infographic.CorporateOverview.pdf) and reports that 14 percent of searches on a branded item lead online users somewhere other than the legitimate brand's site. See also MarkMonitor, "Seven Best Practices for Fighting Counterfeit Sales Online" available at https://www.markmonitor.com/download/wp/wp-Fighting_Counterfeit_Sales.pdf

Counterfeit sellers on large e-commerce platforms are also using social media and email campaigns to drive traffic to their online shop windows. Counterfeiters bury trademark references in lengthy product descriptions, remove logos and trademarks on otherwise recognizable products, blur the trademark from original copyrighted images, or use creative angles to showcase infringing products without running afoul of strictly-construed trademark policies. As one e-commerce submission notes, e-commerce platforms must make continuous efforts to address the ever-more-ingenious techniques for evading detection.

Online counterfeiters enjoy such low operating costs and easy, immediate access to a global customer base that counterfeit goods can be as profitable for criminal gangs as illegal drugs.[16] Retail, luxury brands, electronics, and pharmaceuticals are among the worst-affected sectors. For example, an investment in the trafficking of counterfeit pharmaceuticals can generate a return ten to twenty-five times higher than the same investment in drug trafficking.[17] In addition to counterfeit pharmaceuticals, counterfeit consumer products—such as car parts, children's toys, mobile phones, and sporting equipment—can also endanger consumer health and safety as many counterfeits are made inexpensively with substandard or hazardous materials.[18]

Distribution of counterfeits purchased online from standalone websites and large e-commerce platforms also presents enforcement challenges for rights holders and governments. Instead of shipping a container of counterfeits, today's Internet-facilitated counterfeiters can ship infringing articles one at a time, decreasing the risk of customs detection and minimizing their losses if the shipment is seized. Seizure statistics from U.S. and European customs authorities in the United States and European Union confirm the surge of small consignment shipments. Counterfeiters are also attempting to evade enforcement by shipping trademarked packaging, holograms, and labels separately from the products for later downstream assembly.

USTR applauds governments that are addressing these challenges through legislative, administrative, and executive actions. For example, the European Union recently enhanced its border enforcement authority to address the increase in trafficking of counterfeit goods via small, postal, or express courier consignments.[19]

Provisions in the recently concluded TPP agreement seek to address many of these challenges. These include commitments to provide for criminal procedures and penalties for trafficking in counterfeit labels and packaging; to make enhanced penalties available for particularly serious cases, such as trafficking in counterfeit trademark products that threaten health and safety; to close loopholes used by counterfeiters that threaten global supply chains; and to confirm that enforcement procedures for trademark and copyright infringement are available to the same extent in the digital environment.[20] USTR invites foreign governments to use these and other TPP provisions as a benchmark for addressing online trademark counterfeiting and other 21st century challenges. ■

[16] United Nations Office on Drugs and Crime, Transnational Organized Crime in East Asia and the Pacific, 2013:, available at http://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_EAP_web.pdf (p.128).

[17] International Institute of Research against Counterfeit Medicines, "Counterfeit Medicines and Criminal Organizations," Sept. 2013, at 18 available at http://fightthefakes.org/wp-content/uploads/2013/11/Rapport-Etude_IRACM_Contrefacon-de-Medicaments-et-Organisations-Criminelles_EN_FINALs2.pdf

[18] For a recent example, see "U.S. Customs and Border Protection Holiday Advice for Consumers – Hoverboards" http://www.cbp.gov/newsroom/national-media-release/2015-12-11-000000/us-customs-and-border-protection-holiday-advice

[19] Please see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0479

[20] Visit USTR's TPP resource center for more information at https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-fact-sheets

Results of the 2015 Out-of-Cycle Review of Notorious Markets

As noted, the 2015 List identifies particular online and physical markets in which pirated or counterfeit products and services are reportedly available, but it does not constitute a legal finding or a conclusion as to IPR protection and enforcement in any affiliated country or economy, nor is it intended to be an exhaustive listing of all notorious markets around the world. Rather, the List highlights some of the most prominent examples of both online and physical marketplaces where pirated or counterfeit goods are trafficked that were reported and examined during the OCR process.

Owners and operators of the notorious markets included in the 2015 List that are willing to address piracy and counterfeiting have many options for doing so. Such owners and operators can adopt business models that rely on the licensed distribution of legitimate content and can negotiate appropriate licenses with rights holders. If an otherwise legitimate business has become a platform for piracy or counterfeiting, the owner or operator can work with rights holders and enforcement officials to help discourage and curtail acts of infringement. There are a variety of best practices developed by industries themselves that can help combat these problems. However, in the absence of such good faith efforts, responsible government authorities should investigate reports of piracy and counterfeiting in these and similar markets, and pursue appropriate action against such markets and their owners and operators. Governments should also ensure that appropriate enforcement tools are at the disposal of right holders and government authorities, which may require closing the loopholes that permit operators to evade the law.

Online Markets[21]

The 2015 List of notorious online markets again includes examples of various technologies and business models. USTR based its selections not on specific technologies or business models but on whether, based on available information, a nominated site or affiliated network of sites appears to engage in or facilitate IPR infringement. Accordingly, the 2015 List reflects sites and online services that reportedly engage in and facilitate substantial piracy and counterfeiting to the detriment of U.S. creators and brand owners, as well as legitimate sellers and distributors. In addition to facilitating IPR infringement, these sites may lack safeguards for consumer privacy, security and safety, and some reportedly actively and surreptitiously install malware on users' computers, commit ad-

[21] In most cases, the List identifies online markets by the domain name provided in the public responses to the Federal Register request. However, it is common for operators of online Notorious Markets to change a site's domain name or to use multiple domain names at once to direct users to the main site. The List reflects each market's most commonly referred to or well-known domain name or names as of December 8, 2015.

vertisement fraud, and enable phishing scams to increase their unlawful profits.

4SHARED.COM

With more than 117 million unique visitors a month, this cyberlocker site[22], reportedly based in the British Virgin Islands and hosted in Cyprus, is well-known globally and particularly popular in Brazil.[23] While 4shared provides legitimate services, the site also continues to facilitate streaming and downloads of allegedly pirated videos, music, books and games. By some measurements, 4shared is one of the largest and most profitable direct download cyberlockers that facilitates infringement.[24] 4shared mobile apps further allow users to stream infringing content to mobile devices and recently added search and music player features appear to encourage music infringement. While this site responds to takedown notices, reportedly provides direct access to trusted right holders representatives, and has implemented a feature that scans for unauthorized content, the music industry reports no change in the levels of infringing files.

BUKALAPAK.COM

This consumer-to-consumer marketplace is based in Indonesia and has an Alexa ranking of 12 in that country and 571 globally. While Bukalapak is a platform for legitimate sales, apparel and footwear companies report challenges with counterfeit sellers and a lack of effective procedures for reporting and removing counterfeit listings on this quickly growing e-commerce platform.

[22] The cyberlockers identified in the List reportedly operate primarily to provide users with access to unauthorized content. Such sites are distinguishable from legitimate cloud storage services that allow consumers to lawfully store, share, backup, and access data.

[23] Unless otherwise noted, the global and country-specific popularity of online markets referenced in this List is determined through Alexa rankings, SimilarWeb data, and public submissions. Alexa.com utilizes a proprietary methodology to analyze global and country-specific user traffic and develop a numerical rank that indicates a website's popularity relative to other sites. Rankings can change dramatically and quickly. SimilarWeb.com uses big data technology to estimate websites' unique visitors and the origin of those visits. For example, according to Alexa, 4Shared.com is the 98th most popular website in Brazil and has the highest percentage of global visitors (16 percent) and according to SimilarWeb, 4Shared.com is the 42nd most popular site in Brazil and Brazil has the highest percentage of unique visitors (30 percent). Both the Alexa rankings and SimilarWeb data that appear in this document are current as of December 8, 2015.

[24] NetNames & Digital Citizens Alliance, "Behind The Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions," Sept. 2014, available at http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=cyberlockers. 4shared.com disputes the allegations made in the report.

DHGATE.COM

This Chinese e-commerce site connects Chinese factories and sellers directly with businesses and individual buyers and reportedly hosts over 30 million product listings, some of which allegedly infringe the trademarks and copyrights of U.S. companies. Over the past six years and in each OCR of notorious markets, trademark owners have consistently reported challenges with counterfeits goods on this online wholesale marketplace. Consumer health and safety has been endangered due to counterfeit products that evade detection on the DHgate platform.[25] According to SimilarWeb and Alexa data, DHgate is most popular in China, India, the United Kingdom, Brazil, and the United States.

EBOOKEE.ORG

ALSO OPERATING AS EBOOKEE.DOC.ZZZ.COM

Ebookee is a top indexing site with connections to China that is allegedly dedicated to pirated ebooks, magazines, and other digital media. The site has been operating for more than eight years and provides direct links to files available for download from notorious cyberlockers, some of which, including 4shared and uploaded.net, appear in this List. Along with others, the site and its subsequent variations have been the subject of a court-imposed blocking order in the United Kingdom.

EX.UA AND EXTRATORRENT.CC

These sites, both of which have appeared on the List several times, continue to benefit from Ukraine's status as a haven for online piracy. Almost 35 million users visit EX.UA every month to download and stream content including reportedly infringing music, videos, movies, TV series, e-books, and audiobooks, and software that one commenter alleges is uploaded by site administrators themselves. Similarly, EXTRATORRENT.CC allegedly has extremely high rates of piracy with more than 75 million visits a month and a 14 percent increase in August 2015 compared to August 2014.[26] While Extratorrent has been the subject of successful enforcement actions in several countries, it maintains a global Alexa ranking of 333. Furthermore, Extratorrent has Alexa rankings in India and Pakistan of 76 and 26, respectively, which illustrate the commercial impact that sites which facilitate infringement can have on geographically diverse markets. In 2015, other players in the Internet ecosystem have voluntarily taken reasonable actions against Extratorrent as a result of piracy and malware complaints, including removing search engine access to the site and deleting its social media profile. USTR encourages the Government of Ukraine

[25] Lindsey, Joe "To Catch a Counterfeiter: The Sketchy World of Fake Bike Gear," Bicycling.com, Sept. 15, 2015, available at http://www.bicycling.com/bikes-gear/components/catch-counterfeiter-sketchy-world-fake-bike-gear
[26] According to reported comScore Media Metrix, Word Wide data.

to take lasting action against those who operate these and similar sites within Ukraine's jurisdiction.

KAT.CR

Formerly **KICKASS.TO**, **KICKASSTORRENTS.COM**, and also operated as **KAT.SX**

This BitTorrent indexing site is now the biggest torrent site in terms of visitors and popularity after surpassing ThePirateBay in 2014. KAT.CR has the highest global Alexa ranking of all the online notorious markets on this List. Over 6 million torrent files attracted more than 25 million unique visitors in one month. Reportedly based in Canada, over the past several years the site operators have changed the domain name numerous times, obscured or hidden their locations, and have used multiple servers in various countries to evade or otherwise frustrate enforcement actions. The site originally operated as KICKASSTORRENTS.COM but moved to KAT.PH, until Philippine authorities took enforcement action. The .tt domain registry cancelled the domain KA.TT in 2013, followed by the .so domain registry which cancelled the domain KICKASS.SO in February 2015 and the .im domain registry which cancelled KICKASSTORRENTS.IM in April 2015 within hours.[27] The domain hopping tactics deployed by KAT.CR allow the site to reappear at the top of search results and evade court-ordered injunctions.

MOVSHARE GROUP

OPERATING AS NOWVIDEO.SX, WATCHSERIES.IT, TORRENTZ.EU, VIDEOWEED.ES, NOVAMOV.COM, AMONG OTHERS

This group of affiliated and extremely popular sites, with ties to Switzerland, Sweden, the Netherlands, Panama, Canada, and other countries, reportedly uses multiple technologies to make available countless unauthorized copies of movies, games, music, audiobooks, software, and sporting event broadcasts. These cyberlockers, linking sites, forums, and streaming sites all work together to facilitate global distribution of allegedly infringing content. The sites are said to generate revenues through advertising and premium membership or subscription fees, and to compensate users for uploading infringing content. Rights holders report that Nowvideo and others in the Movshare group are systematically unresponsive to takedown notices.

[27] .tt is the country code top-level domain (ccTLD) of Trinidad and Tobago, .so is the ccTLD of Somalia, and .im is the ccTLD of Isle of Man.

PRIVATE LAYER-HOSTED SITES

PUTLOCKER.IS, **CUEVANA.TV**, WATCHSERIES.IT, and NOWVIDEO.SX (listed as part of the Movshare Group)

This group of websites, all hosted by Private Layer based in Switzerland and Panama, are evidence of the rising popularity among pirate sites of certain Swiss hosting services. Switzerland has announced plans to close a loophole in its law that restricts enforcement against pirate sites. However, at this time, rights holders report that Switzerland is an increasingly popular host country for such sites. PUTLOCKER.IS returns to the List after re-building its user base and rising in the ranks to once again become a globally popular site for allegedly pirated movies and television shows. The operator of Putlocker is based in Vietnam. Another streaming site based in Argentina, CUEVANA.TV, attracts large numbers of Spanish-speaking users from Argentina, Mexico, Spain, and Chile.

REBEL

A **DIVISION OF MOMENTOUS**

This Canada-based domain name registrar allegedly knowingly licenses domain names to a disproportionate number of illegal online pharmacies. Rebel maintains less than 0.05 percent of the total domain name market but reportedly more than 17 percent of the entire illegal online pharmacy market.[28] One submission estimated that Rebel sells domain name registration services to 4,850 illegal online drug sellers.[29] Private organizations and regulatory authorities have notified Rebel of the illegal nature of the online pharmacies it sponsors but Rebel has reportedly not taken action and has allegedly become a "safe haven" for criminal enterprises specializing in counterfeit drugs.[30] This year's submissions reflect that, while the role of domain name registrars remains an ongoing subject of important discussion, Rebel's outlier status is evidence that it is not taking measures that other domain name registrars have found to be reasonable to address infringement, such as having policies that prohibit domain names from being used in furtherance of criminal activity and acting on complaints as appropriate to suspend or lock domain names of illegal online pharmacies.

[28] United States. Cong. House. Subcommittee on Courts, Intellectual Property and the Internet. Stakeholder Perspectives on ICANN. Hearings, May 13, 2015. 114th Cong. 1st sess. (testimony of John C. Horton) available at http://judiciary.house.gov/_cache/files/479d5a53-11d3-4919-80fb-e8e24d462cbf/legitscript---john-horton---house-judiciary-commitee-testimony---05-13-15.pdf

[29] Previously-listed domain name registrar **Tucows** was again nominated this year. Illegal online pharmacies reportedly continue to obtain domain names from Tucows.

[30] Consumer information regarding online pharmacies is available from the U.S. Food and Drug Administration's through the BeSafeRx campaign (http://www.fda.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicineSafely/BuyingMedicinesOvertheInternet/BeSafeRxKnowYourOnlinePharmacy/) and Know Your Source campaign (http://www.fda.gov/Drugs/ResourcesForYou/HealthProfessionals/ucm389121.htm) as well as at the following websites: http://safeonlinerx.com; www.safemedsonline.org; and www.nabp.net/programs/accreditation/vipps While these sites focus primarily on the U.S. audience, similar resources are available to consumers outside the United States, including at http://asop.eu/home

RAPIDGATOR.ORG AND RUTRACKER.ORG

Formerly **TORRENTS.RU**

Commenters from the book publishing, movie, entertainment software, and music industries all nominated Rapidgator for inclusion on this year's List. Rapidgator is hosted in Russia but primarily provides allegedly infringing content to users outside of the country. RAPIDGATOR.NET employs rewards and affiliate schemes to compensate users based on downloads and sales of new accounts. Operators of the site allegedly net an estimated $2 million annually.[31] RUTRACKER.ORG, hosted in and operated from Russia, is a BitTorrent portal with more than 13 million active accounts. The site is currently one of the most popular in the world and a top site in Russia. Ongoing court action in Russia may result in decreased use of the site, but that court action is not final.

SEGUNDAMANO.ES

Also operating as **VIBBO.COM**

This site is the most popular example of a circumvention device distribution website that allegedly facilitates the unauthorized use of copyright-protected games by selling "mod chips" or game copier hardware that are used to circumvent technological protection measures designed to promote authorized uses. Segundamano is based in Spain.

UPLOADED.NET

Also operating as **UL.TO** and **UPLOADED.TO**

This cyberlocker with alleged connections to Switzerland and Netherlands, provides access to a broad range of unauthorized copies of copyright-protected content, provides a reward system to its users, and reportedly generates over $6 million per year in advertising and subscription revenues. The site operator allegedly employs multiple IP addresses, domain names, and server locations to evade law enforcement. The site is popular around the world and undermines the market for legitimate content in Japan, Germany, France, Spain, and the United States, sometimes before the content has even been released.

VK.COM

Also known as **VKONTAKTE.COM**

Nominated again this year, VK.COM is one of the most popular sites in the world and continues to operate as an extremely popular social networking site in Russia and neighboring countries. VK.COM reportedly facilitates the distribution of allegedly infringing mov-

[31] NetNames, Behind the Cyberlocker Door, 28.

ie, television and music files. Social networking sites can serve as a uniquely valuable communication platform, enabling beneficial commercial, cultural, and social exchanges. Most successful social networking sites do so in ways that do not involve the active facilitation of copyright infringement. Reports that VK.COM is taking steps to address piracy are encouraging, and the United States hopes to see measurable and lasting measures comparable to other social media sites.

ZIPPYSHARE.COM

Well-known for downloads and distribution of allegedly infringing music, Zippyshare allegedly offers more pre-release music, i.e. music that has not yet been commercially released, than any other cyberlocker. Zippyshare is reportedly hosted in France. Its revenues reportedly come from paid advertising, which targets millions of users from around the world, particularly from India, where the site has an Alexa ranking of 278. Zippyshare pages are known to install malware on visitors' computers and send visitors to dangerous websites.[32]

Physical Markets

The Internet has brought about a global revolution in the authorized and unauthorized distribution of films, music, software, video games, and books. In many markets, unauthorized online distribution of, or access to, copyright-protected content largely has replaced unauthorized distribution via physical media. In other markets, however, physical media (including CDs, DVDs, video game cartridges, and pre-loaded computer hard drives and other storage devices) continue to be prevalent, with widespread distribution, at times involving local manufacture, through markets such as those identified below.

The Internet also makes available innumerable sites that facilitate the distribution of counterfeit products to consumers worldwide. However, physical markets, such as the ones listed below, remain the primary distribution channel for counterfeit goods in much of the world.

In a global environment, enforcement against unscrupulous retailers, although important, will not be sufficient to reduce the flow of counterfeit products. Enforcement tools, such as asset forfeiture, can help target custodians of locations that sell and store infringing products. The importance of effective border enforcement measures to prevent the exportation of counterfeit goods from their countries of manufacture, the importation into the destination country, and the transiting of such goods through third countries on their way to destination countries cannot be overstated. Another key to reducing piracy and counterfeiting, however, lies in the ability to influ-

[32] Safe Browsing Site Status, Google Transparency Report available at https://www.google.com/transparencyreport/safebrowsing/diagnostic/?hl=en. As of December 8, 2015, ten of the online markets on this List were identified as sending visitors to dangerous websites, four were identified as installing malware on visitors' computers, one site was identified for trying to trick visitors into installing programs that harm their browsing experience, and dangerous websites were sending visitors to at least four of the listed sites.