RIAA Submission to Comment Request for the
2020 Review of Notorious Markets for Counterfeiting and Piracy
Docket No. USTR-2020-0035
November 8, 2020
Submitted via regulations.gov

The Recording Industry Association of America (RIAA) welcomes the opportunity to provide this submission in response to your request for comments identifying online and physical markets to be included in the 2020 Review of Notorious Markets for Counterfeiting and Piracy.

INTRODUCTION

The RIAA is the trade organization representing major U.S. music companies. RIAA's members create, manufacture, or distribute sound recordings representing approximately 85 percent of all legitimate recorded music consumption in the United States.

The RIAA appreciates that the "United States encourages owners and operators of markets reportedly involved in piracy of counterfeiting to adopt business models that rely on the licensed distribution of legitimate content and products to work with rights holders and enforcement officials to address infringement."[1] The U.S. recorded music industry is highly reliant on intellectual property in order to drive innovation, creativity, and growth within this sector, and to enforce against those that unfairly and illegally steal our members' music for their own pecuniary interests.

The music industry contributes significantly to the U.S. economy and to U.S. trade exports. For example, the music industry is a leader in driving digital commerce, including by helping to fuel the growth of the streaming economy. Streaming music grew to 85% of the total music market by value, while physical products amounted to about 7%.[2] In addition, as noted in a 2018 report, the music industry, collectively with other creative industries, supports 5.7 million American jobs, and contributes $1.3 trillion to the U.S. GDP.[3] Furthermore, U.S. intellectual property licensing, of which music is a part, contributed $117.4 billion in services exports in 2019, resulting in a net services trade surplus of over $74.4 billion for this category during this period.[4] Even during the pandemic, between January and September of 2020,

[1] 85 Fed. Reg. 62007 (October 1, 2020).
[2] Source: RIAA. See https://www.riaa.com/reports/2020-mid-year-music-industry-revenue-report-riaa/.
[3] Siwek, Stephen, "Copyright Industries in the U.S. Economy: The 2018 Report" prepared for the International.
Intellectual Property Alliance (IIPA); December 6, 2018.
[4] Source: U.S Census Bureau and the U.S. Bureau of Economic Analysis, "MONTHLY U.S. INTERNATIONAL TRADE IN GOODS AND SERVICES, SEPTEMBER 2020," Release Number: CB 20-

intellectual property licensing contributed $80 billion in services exports, resulting in a net services trade surplus of over $49 billion for this category during this period.[5]

However, in inflation-adjusted dollars, our industry's revenues in the first half of 2020 only represent 50% of our peak U.S. revenues from 1999.[6] This period of time coincides with the rise of digital piracy generally, and the later rise of the sale and importation of foreign-made, counterfeit physical music products though ecommerce platforms. Moreover, the Covid-19 pandemic has impacted the U.S. music industry, as shown in differences in revenue trends between Q1 and Q2 of 2020,[7] including with respect to tour cancellations, retail store closures, the reduction in online advertising, and the emergence of illegitimate live streaming for music consumption.

In this submission, we first address online markets engaged in or facilitating copyright policy, followed by physical markets engaged in or facilitating copyright piracy. We then address the issue focus for 2020, namely ecommerce platforms and other third-party intermediaries.

ONLINE MARKETS ENGAGED IN OR FACILITATING COPYRIGHT PIRACY

The following is a list of online markets that engage in or facilitate substantial copyright piracy that infringes on U.S. intellectual property. We request these markets be considered for inclusion in the 2020 Notorious Markets List. These markets engage in the unlicensed sale, streaming, and/or distribution/downloading or other unauthorized dissemination of sound recordings that significantly damage the rights of U.S. companies, and/or also engage in circumvention activities that violate 17 USC § 1201.

These services harm U.S. artists, record labels, and music publishing companies by (i) disseminating music without authorization and without providing any compensation to the creators and owners of the music, and (ii) artificially distorting the market value of the music, thereby reducing the compensation to the creators and owners from licensed services.

Many of the services disseminating infringing content that we have included in this year's submission regrettably have been included in the past. While some of these sites have made incremental changes to the way they operate to limit some of their exposure to liability, unfortunately the traffic to these sites remains high and the damage inflicted on the U.S. recording industry is immense.

The U.S recorded music industry continues to engage in various forms of "self-help" to address this infringing activity, including sending traditional infringement notices, warning

---

166, BEA 20-55, Nov. 4, 2020, exhibits 3 and 4. See https://www.census.gov/foreign-trade/Press-Release/current_press_release/ft900.pdf, https://www.census.gov/foreign-trade/Press-Release/current_press_release/exh3.pdf and https://www.census.gov/foreign-trade/Press-Release/current_press_release/exh4.pdf.

[5] Id.

[6] Source: RIAA. See also Smith, Dylan, "Despite Streaming, US Recorded Music Revenues still down 50% from 1999 Peaks", Digital Music News, August 27, 2020, available at https://www.digitalmusicnews.com/2020/08/27/recorded-music-revenues-decrease/.

[7] Id.

letters, and cease and desist letters, and engaging in civil litigation and criminal enforcement referrals where sites refuse to respond. These actions, along with efforts to highlight the problems through government action, such as through the Notorious Market Report, have been helpful in informing third-party intermediaries such as hosting providers, advertisers, and payment providers, and in some cases modifying the behavior of online services.

However, we continue to face significant challenges in our investigation and enforcement efforts. One challenge we face is that the sites that have shut down can reappear as quickly as they disappeared. In some cases, they reemerge with the same second-level domain name but on a different top-level domain, from the same hosting Internet service provider (ISP), and with the same functionality (what we call domain-hopping). In other instances, they return with slightly altered domain names with new hosting ISPs, new registrars, and/or new registrant information. We also often see "copycat" infringing services pop up as well. In fact, infringing operations these days are often multi-jurisdictional and based on complex, dynamic structures involving various types of third-party intermediaries. Such complex and dynamic structures are often deliberate as they increase the time, cost, and difficulty of enforcement action, and thus reduce the likelihood that effective action can be taken against the operators. The dynamic and low-cost nature of the Internet presents unique challenges in comprehensively identifying and addressing notorious markets.

In addition, in today's environment, it has become exceedingly difficult to track, enforce against, and accurately associate various notorious websites because of, among other things:

- **Severely Restricted Access to Domain Name Registration Data** – Domain Name Registration Data has been severely and overly restricted by ICANN and the registrars and registries in their quest to reduce their liability risk under the European Union's General Data Protection Regulation. Despite promises to establish and implement a policy to provide uniform and consistent rules on how users can access such registration data, including for intellectual property protection and enforcement purposes, ICANN has yet to fully develop or implement such rules.[8] As previously noted, this continues to frustrate our ability to contact the registrant directly to address infringement issues, investigate relationships between infringing sites, and analyze our other enforcement options.[9]

- **Privacy/Proxy Protected Domain Name Registration and False Domain Name Registration Data** – In addition, operators of pirate sites typically hide their identity behind privacy/proxy services or appear to submit false or incomplete registrant information, further creating obstacles to enforcement against these sites. Despite ICANN having a fully approved, bottoms-up, multi-stakeholder policy to require privacy/proxy service providers to disclose true registrant data in cases of clear,

[8] See, e.g., letter from Manel Ismael, Chair of the Governmental Advisory Committee (GAC) of ICANN to Keith Drazek, Chair of the GNSO Council of ICANN, dated June 20, 2020 (GAC June 20, 2020 letter), documenting issues yet to be addressed, available at https://gac.icann.org/contentMigrated/next-steps-on-key-policy-issues-not-addressed-in-epdp-phase-2. See also the ICANN 69 GAC Communique to ICANN dated October 23, 2020, available at https://gac.icann.org/contentMigrated/icann69-gac-communique.

[9] It also leads to increased problems with cybersecurity threats and brand protection concerns. See, e.g., Vayra, Fabricio, *The End of the Road: ICANN, WHOIS, and Regulation*, Circle ID, September 25, 2019, available at http://www.circleid.com/posts/20190925_the_end_of_the_road_icann_whois_and_regulation/.

infringing activity, ICANN continues to delay implementation of that policy.[10] With estimates of over one third of all domain name registrations behind a privacy/proxy service, this failure of ICANN to implement disclosure policies for privacy/proxy services only serves to embolden online infringers and others that engage in malicious activity online with only minimal risks of identification and reprisal. In addition, ICANN has failed to adopt meaningful solutions to improve the accuracy of registrant information, despite discussions on this topic for the last several years.[11]

- **Prevalent Use of Reverse Proxy Services to Obfuscate Hosting ISP** – These services are utilized by pirate websites to hide the identity and location of actual hosting ISPs. While reverse proxies can provide valuable service to protect legitimate websites from attack and provide other important services, more and more pirate sites employ reverse proxy services to hide their true IP address from rights holders, thus creating obstacles to enforcement against such sites.

- **Use of "Bulletproof" ISPs** – Several infringing sites use off-shore hosting ISPs that support the sites' infringing activities. These "bulletproof" ISPs support various types of criminality through considerable leniency in the kinds of materials they permit to be uploaded and distributed via their networks. These ISPs do not respond to notices of infringement or warning letters that the ISP is hosting and supporting known infringing sites.

In fact, there are thousands of websites on the Internet that are dedicated to piracy, with new ones appearing all the time and existing ones frequently changing their online location (whether domain or hosting environment, or both) to avoid enforcement. This list of notorious markets is therefore by no means comprehensive. We focus instead on those sites and services that inflict the most damage on the U.S. recording industry, either globally or in specific country markets.

We monitor traffic to the sites using Alexa.com for overall global rankings and SimilarWeb, a web traffic analytics company, to track website visits. The ranking and traffic data used in this submission is based on the data available through September 2020 from these two sources.

1. Stream-ripping Sites

As noted in the 2020 Special 301 Report, "[s]tream-ripping, the unauthorized converting of a file from a licensed streaming site into an unauthorized copy, is now a dominant method of music piracy, causing substantial economic harm to music creators and undermining legitimate online services."[12]

[10] See September 5, 2019 letter from ICANN to Keith Drazek continuing the delay of implementation of the privacy/proxy services approved policy, available at https://www.icann.org/en/system/files/correspondence/namazi-to-drazek-et-al-05sep19-en.pdf. See also the ICANN 68 GAC Communique to ICANN dated June 27, 2020, available at https://gac.icann.org/contentMigrated/icann68-gac-communique.
[11] See, e.g., GAC June 20, 2020 letter.
[12] 2020 Special 301 Report, April, 2020, p. 22, available at https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf.

The unauthorized distribution of permanent downloads of files from streaming services deprives the record companies and artists of streaming revenue by eliminating the need for users to return to YouTube and other licensed services every time they listen to the music. They harm ad-based streaming services by enabling users to listen to their favorite recordings over and over again without generating ad revenue for the artists and labels. They undermine premium streaming services that offer tethered downloads for off-line listening. Stream-ripping services also undercut pay-for-download sites like iTunes and Amazon by providing permanent downloads for free. The overall popularity of these sites and the staggering volume of traffic they attract evidence the enormous damage being inflicted on the U.S. record industry.

Several countries around the world have found these stream-ripping services to be unlawful.[13] Several stream-ripping services have also shut down after a demand or lawsuit from the record companies. Unfortunately, however, new or variant stream-ripping services rise up to take their place. According to SimilarWeb stream-ripping sites we are tracking have generated 10.4 billion visits globally, and 1.1 billion visits in the U.S. over the last 12 months.

We are currently tracking more than 200 active stream-ripping sites. The most popular and, hence, the most damaging of these stream-ripping sites are:

Ytmp3

Domain: ytmp3.cc (formerly youtube2mp3.cc)
Registrant: Uses privacy/proxy service Global Domain Privacy Services, Panama
Registrar: Pananames - URL Solutions, Panama
Hosting Provider: Servers.com and United Network, LLC, both in Moscow, Russian Federation; backend content servers – OVH (France)
Traffic: Global Alexa ranking of 515, with over 1.4 billion visits in the past 12 months, up from 1.2 billion last year
Revenue Source: Advertising

Ytmp3's user-facing front-end site is hosted in Russia and describes its service as providing a converter where the user "can easily convert YouTube videos to mp3 (audio) or mp4 (video) files and download them for free." To obtain a copy of a YouTube video, the user simply pastes a YouTube video URL into the converter bar, chooses a format (audio only or full video file) and clicks the convert button. When the "conversion" is completed, the user can download the file by clicking on the download button. It appears that the service does not actually convert each URL on demand, but rather retains copies of files previously converted on backend servers hosted on OVH (France) to maintain a more efficient and reliable service.

Mp3juices

Domain: mp3juices.cc
Registrant: "Redacted for Privacy"
Registrar: Tucows (Canada)
Hosting Provider: Servers.com and United Network, LLC, both in Moscow, Russian

[13] Source: IFPI; see https://www.ifpi.org/italian-court-confirms-stream-ripping-is-illegal/.

Federation; backend content servers – OVH (France)
Traffic: Global Alexa ranking of 4355, with nearly 1.15 billion visits in the past 12 months, down just slightly from last year
Revenue Source: Advertising

Mp3juices appears to be connected to *ytmp3.cc* as both sites have historically been hosted on the same ISPs, and both use a separate back-end domain to copy, store, and deliver the infringing files to users. Content accessed through *mp3juices* is also delivered through frequently changing backend domains that have also operated with the same registrant information, registrar, and hosting provider as *ytmp3*. *Mp3juices* differs from *ytmp3* only in that it offers the YouTube search capability directly from its homepage and that eliminates the need to cut and paste the YouTube URL into a conversion bar. *Mp3juices* also provides only mp3 audio files of the YouTube video and does not offer an option to download the entire video. Like *ytmp3*, it appears that the service does not actually convert each URL on demand, but rather retains copies of files previously converted on backend servers.

Flvto & 2Conv

Domain: flvto.biz and 2conv.com
Registrant: Currently "Redacted for Privacy" but previous proxy service identified registrant for both sites as Tofig Kurbanov, Russian Federation
Registrar: Nicenic International Group (Hong Kong)
Hosting Provider: Both sites now hosted on Upcloud, Ltd. (Finland)
Traffic: Flvto.biz has a global Alexa Ranking of 1391 and 2conv.com has a global Alexa ranking of 2876; collectively, the two sites have had over 1.14 billion visits in last 12 months
Revenue Source: Advertising and questionable software downloads

Flvto.biz and *2Conv* are operated by the same individual in Russia and serve downloads of converted YouTube videos to users as digital audio files. All the user needs to do is to copy and paste a YouTube link into a conversion bar and click on a "convert to" button. These sites are dedicated to the mass-scale piracy of our members' copyrighted sound recordings that are available on YouTube. Following some of our enforcement activity, the sites changed their operations slightly, but nonetheless continue to engage in unauthorized distribution of our members' music. We also have reason to believe that the operator may be involved in other stream-ripping sites as well.

U.S. record companies filed a lawsuit against these sites in 2018 in the United States District Court for the Eastern District of Virginia, alleging copyright infringement on a massive scale. The court granted the Russian defendant's motion to dismiss for lack of personal jurisdiction, despite substantial facts that support jurisdiction over the defendant in the United States. The decision was overturned on appeal to the United States Court of Appeals for the Fourth Circuit earlier this year and remanded back to the district court. The defendants have filed a cert petition with the Supreme Court.

Y2mate

Domain: y2mate.com (and related site youtubeconverter.io)
Registrant: Uses privacy proxy service Whois Privacy, Panama; registrant believed to be Ken Nguyen, Hanoi, Vietnam
Registrar: NameCheap, Inc.
Hosting Provider: Hetzner Online GmbH, Germany, through Cloudflare (US)

Traffic: Global Alexa ranking of 233, with nearly 1.65 billion visits in the past 12 months
Revenue Source: Advertising

Y2mate offers a search capability to locate YouTube videos or allows the user to cut and paste a YouTube URL into the search bar. Users are enabled to download either an audio-only mp3 or the entire audio-visual work as an mp4 file. The site also appears connected with the stream-ripping site *youtubeconverter.io* and provides users with a link to this service if they are unable to download the mp3 file via *y2mate*.

Savefrom

Domain: savefrom.net
Registrant: Domains By Proxy
Registrar: GoDaddy (US)
Hosting Provider: Online SAS (France)
Traffic: Global Alexa ranking of 142 with over 1.6 billion visits globally in the past year
Revenue Source: Advertising

Savefrom.net operates with a slightly different but equally damaging model. Rather than downloading content to their servers and then offering mp3s or full videos for download, *Savefrom* simply circumvents the YouTube content protection measures and serves up the unprotected content directly to users from the YouTube servers where the user can either save the video or save the audio to their devices. Earlier this year, *Savefrom* announced that, due to "strenuous attacks by certain US copyright holders," it was terminating its services in the United States. *Savefrom*, however, has continued to function in many jurisdictions outside the U.S. and continues to generate in excess of 120 million visits a month to its site globally.

MP3-YouTube

Domain: mp3-youtube.download
Registrant: Last publicly available information – Hedi Chaibi, Roubaix, France
Registrar: OVH SAS
Hosting Provider: OVH SAS, France
Traffic: Global Alexa ranking of 1301, with over 700 million visits in the past year
Revenue Source: Advertising

As its name implies, *mp3-youtube* offers users the ability to convert a YouTube video to a free downloadable mp3 audio file. The site touts that "there is no simpler and faster youtube converter: you just paste the video URL link you want to download…and a few seconds later you get an mp3 in original quality." Its homepage goes on to boast that its "youtube mp3 converter is not only able to download videos from Youtube to mp3, but is also compatible with the most popular websites: Facebook, Vimeo, Soundcloud, Instagram, etc."

2. Mp3 Search-and-Download Sites

This class of sites directly or indirectly offers unauthorized on-demand streaming and/or downloading of our members' music, including their most popular and valuable content. Commonly, these sites also provide unauthorized downloading of pre-release music, i.e., tracks and albums that have not yet been commercially released to the public. As noted

above, such infringing activity clearly harms U.S. artists, songwriters, record labels, and music publishers by disseminating their works without authorization and severely diminishing the commercial value of those works.

Newalbumreleases

Domain: newalbumreleases.net
Registrant: Uses privacy/proxy service Super Privacy Services, last identified registrant believed to be Sergey Kobilin, Svetogorsk, Russia
Registrar: Dynadot, LLC
Hosting Provider: Served through Cloudflare (US), underlying ISP believed to be WIBO (Czech Republic)
Traffic: Global Alexa ranking of 39,939, with nearly 25 million visits in the past year
Revenue Sources: Advertising

Newalbumreleases makes available a substantial library of newly released popular music content, as well as albums not yet commercially released. The site features the most recently uploaded albums on the homepage using album artwork. In addition, it organizes earlier posts by genre under menu tabs for Rock, Pop, Metal, etc. The homepage also offers a search capability for content by artist or title. The site hosts its content on cyberlockers and provides users with links to services like *Rapidgator.net* and *Turbobit.net* from which the files are available for download. All the files appear to have been uploaded to the cyberlocker sites by *Newalbumreleases*, as the download files usually include "newalbumreleases" in the file name. As the uploaders of the files, *Newalbumreleases* are direct infringers. Takedown notices sent by rights holders to this site are ineffective.

Rnbxclusive

Domain: rnbxclusive.vip (previous iterations include rnbxclusive.com, rnbxclusive1.com, rnbexclusive.best, and rnbxclusive.live)
Registrant: Uses privacy/proxy service WhoisGuard
Registrar: Namecheap, Inc
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Contabo GmbH
Traffic: Global Alexa ranking of 164,912, with over 1.4 million combined visits to this site at its various domains in the past year
Revenue Sources: Advertising

Rnbxclusive is a popular Ukrainian-based service providing downloads for popular R&B and Hip-hop recordings, both full albums and popular tracks for free download. The site uses various problematic cyberlockers, like *turbobit.net* to host and distribute the files. The site has also been a prolific domain-hopper, having hopped domains approximately 16 times since 2016.

Leakthis

Domain: leakth.is
Registrant: Not publicly disclosed
Registrar: Unavailable
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Amanah Tech Inc. (Canada)
Traffic: Global Alexa ranking of 34,124, with over 12.5 million visits to the site in the past year

Revenue Sources: Advertising

Leakthis is, as its name implies, a site that specializes in the most damaging forms of piracy, which is the leaking of tracks and albums before their commercial release. The site itself is not a massively popular site, but it is the source of content that, once leaked, rapidly spreads across the entire music piracy landscape. Thus, its damage is measured not in how many users visit the site itself but by the massive distribution of unlawful pre-release content that takes place once the file is made available on the site.

Intmusic

Domain: intmusic.net
Registrant: Whois Privacy Corp (Private Registration)
Registrar: TLD Registrar Solutions, Ltd.
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be NForce Entertainment B.V (Netherlands)
Traffic: Global Alexa ranking of 409,620, with 9.6 million visits in the past 12 months
Revenue Sources: Advertising

Intmusic makes available large amounts of newly released popular music content, as well as music that has not yet been commercially released. The site features a fully searchable index with each post categorised by genre and provides numerous download links to cyberlockers such as *Rapidgator*. *Intmusic* is non-compliant to takedown notices.

Pluspremieres

Domain: pluspremieres.to
Registrant: Not Publicly Disclosed
Registrar: Namecheap, Inc
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Google LLC (United States)
Traffic: Global Alexa ranking 27,977 with 4.2 million visits in last12 months
Revenue Sources: Advertising

Pluspremieres offers users the option to download from a large variety of unauthorised music sound recordings including pre-release/unreleased content. The site allows users to browse and search by content category including music genre. Each post on the site provides download links to various cyberlockers including *ddownload.com* and *zippyshare.com*, as well as the ability to share links with other users. Metadata relating to the content is also made available, including the genre and release information and track listings. *Pluspremieres* remain non-compliant with takedown requests and the site is fully ad-supported.

AK47Full

Domain: ak47full.com
Registrant: Privacy Protect, LLC (PrivacyProtect.org) - Private Registration
Registrar: Shinjiru Technology
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be OVH SAS (France)
Traffic: Global Alexa ranking 27,588 with 16.1 million visits in the past 12 months
Revenue Sources: Advertising

Ak47full provides users with multiple options for downloading unauthorised audio recordings. On the homepage, a search bar is provided as well as a dropdown "Music" tab with various options including "New Releases," "New Releases USA," "Album," etc. There is also a section on the homepage for "Most Seen" and "New Albums." Once selected, the content downloads directly from the site itself to the user's computer at the click of the

download button. The site also provides users with the option to further distribute the content via social media.

Kingdom-Leaks

Domain: kingdom-leaks.com
Registrant: Uses privacy/proxy service WhoisGuard
Registrar: Namecheap, Inc
Hosting Provider: Frantech Solutions (USA)
Traffic: Global Alexa ranking 64,213, with 6.5 million visits in the past 12 months
Revenue Sources: Advertising and user donations

Kingdom-leaks is, as its name implies, a site that specializes in the most damaging forms of piracy, which is the leaking of tracks and albums before their commercial release. The site itself is not a massively popular site, but it is the source of content that, once leaked, rapidly spreads across the entire music piracy landscape. Thus, its damage is measured not in how many users visit the site itself but by the massive distribution of unlawful pre-release content that takes place once the file is made available on the site.

3. BitTorrent Indexing Sites

BitTorrent indexing sites provide a searchable index of links to content which can be downloaded by users running the appropriate client software. Indexing services can generate revenue from advertising and/or user donations. The financial model, structure, and approach varies from site to site.

The following popular sites are the most egregious, based on: (i) the extent of the infringement, i.e., the number of users visiting the site to infringe copyright; (ii) the amount of unlicensed content on the site; and (iii) the site's failure to take steps to address the massive piracy problem across its network. Moreover, these BitTorrent index sites demonstrate they are dedicated to infringement by the way they organize and display the files they index. Files are typically organized into categories of movie, music, software, and games with file names clearly and unmistakably describing content in a way that the operators know they are distributing torrents for copyright-protected content.

Increasingly, BitTorrent sites are registering multiple domains to mitigate the problem of their sites going offline if one of their domains is seized or blocked, and to work around search engine demotion algorithms. A simple change in the county code or other top-level domain allows the site to reappear in top search results.

ThePirateBay

Domain: thepiratebay.org (formerly thepiratebay.se, thepiratebay.vg)
Registrant: Fredrik Neij, Stockholm, Sweden
Registrar: easyDNS Technologies Inc.
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Lir.bg EOOD, Bulgaria
Traffic: Global Alexa ranking of 169, with nearly 686 million visits in the past year; this figure does not capture the myriad of mirror sites that are constantly being generated to get around blocking orders against the site from numerous countries around the world

Revenue Sources: Advertising, pay-per-install of potential malware

Thepiratebay remains the single most popular BitTorrent index site in the world. This continues to be the case even though courts in a multitude of countries around the world (including Austria, Belgium, Denmark, Finland, Iceland, Ireland, Italy, Portugal, Spain, and the UK) have issued orders blocking access to the site in their jurisdictions. Earlier this year, *thepiratebay* began blocking U.S. IP addresses. However, the site remains easily accessible using a free proxy service that makes it appear the user is accessing the site from another jurisdiction. The world's most popular and newly released films and vast catalogues of music can be downloaded via the site. The site makes no pretense of legitimacy, fails to respond to any takedown notices, and has previously ridiculed those who have sent them such notices.

There are a number of other very popular BitTorrent index sites that operate in essentially the same fashion as *thepiratebay*, making a broad range of copyrighted content downloadable using the BitTorrent P2P protocol. The worst of these sites includes:

1337x

Domain: 1337x.to and mirrored at 1337x.tw (site previously used 1337x.se, 1337x.st, x1337x.ws, x1337x.eu, and x1337x.se)
Registrant: None provided for .to TLD
Registrar: Epag Domain Services, GMbH
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be the bulletproof ISP FlokiNet, Ltd.
Traffic: Global Alexa ranking of 344, with nearly 710 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

Rarbg

Domain: rarbg.to
Registrant: None provided for .to TLD
Registrar: Not available
Hosting Provider: Nets App/S A and A Stroi Proekt EOOD, Bosnia and Herzegovina
Traffic: Global Alexa ranking of 262, with 1.5 billion visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

Torrentz2

Domain: torrentz2.eu (mirror or copycat sites may include torrentz2eu.xyz, torrentz2.is)
Registrant: None provided for .to TLD
Registrar: Not available
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Private Layer, Inc.
Traffic: Global Alexa ranking of 573, with 547 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware

4. Cyberlockers

A "cyberlocker" is a type of website/service which enables users to upload, store, and distribute digital files on a dedicated storage infrastructure on the Internet that is controlled, managed, and maintained by the website's operator. Although there appears to be some similarity between cyberlockers and legitimate cloud storage services (as they both allow users to upload files to servers for storage and sharing), their business models are strikingly different. The business model for legitimate storage services is principally based around personal file storage and limited ability to share access to the files. Cyberlockers are all about maximizing and monetizing traffic to their service. Nothing draws traffic like popular copyrighted content that can be downloaded for free. Thus, their business model is, at its heart, the distribution of unlicensed content.

Cyberlockers typically earn revenue from one or more of the following means: advertising such as banner and "pop-up" ads, which usually appear on the pages where the files to be downloaded are accessed; and sale of "premium accounts," which offer users benefits such as greatly increased download speeds, no-wait downloads, and simultaneous downloads – all features of particular interest to users who want to download large files such as films and albums. Some cyberlockers provide financial rewards to uploaders whose content draws large volumes of traffic to the site (which translates to advertising dollars) or when a downloader purchases a premium account after accessing an uploader's content. Conversely, cyberlocker sites often have a policy of deleting content uploaded by non-paying users that is not regularly downloaded by others – in other words, content which is not drawing traffic to the site. Finally, these services provide little if any accountability for infringing uploaders. Files can often be uploaded without even opening an account, or free accounts can be opened with nothing more than an email address. Thus, there is no ability to police uploaders or effectively remove repeat infringers from their system. The fact of the matter is that, for many of these services, there would be no economic viability in the absence of traffic generated through piracy.

To a limited extent, rights holders can attempt to tackle these infringements by sending takedown notices to the site operators. However, this often entails monitoring thousands of third-party link resources – e.g., blogs, forum sites, and search engines – to locate the information that is needed to notify the locker of infringements occurring on their own services. These services are in a much better position to identify infringing content being uploaded to or distributed from their own servers if they really had an interest in conducting their business legally. There are efficient and reasonable technological solutions available that would assist in this.

The following are some of the most problematic cyberlocker sites plaguing the U.S. music industry:

Zippyshare

Domain: zippyshare.com
Registrant: Uses privacy/protection service Contact Privacy Inc. (Canada)
Registrar: Tucows Domains Inc. (Canada)
Hosting Provider: OVH SAS (France)
Traffic: Global Alexa ranking of 491, with 634.4 million visits in the past year
Revenue: Advertising, pay-per-install of third-party applications

Zippyshare is operated by an individual in Poland, has particularly high traffic, and is notably used for downloads of infringing music over other forms of content. Like other cyberlockers, it generates shareable URLs to content uploaded to its servers by users and, when those URLs are accessed, it makes those files available to download or stream via an embedded music player. Its revenue is derived primarily from advertising (notably it does not offer reward schemes or premium accounts). While the site responds to takedown notices, it permits the anonymous upload of content to the site, so there is no way to screen out those who abuse the service or simply repeatedly re-upload content that was previously removed. The Google Transparency Report reveals (as of September 2020) that Google has received notices to delist over 14 million *Zippyshare* URLs from its search results. Proceedings alleging that the site is directly liable for copyright infringement are currently underway before the High Court of England and Wales.

Rapidgator

Domain: rapidgator.net (and rg.to, which redirects to rapidgator.net)
Registrant: Uses privacy/proxy service Whois Privacy Corp., Nassau, Bahamas
Registrar: Internet.BS Corp.
Hosting Provider: NetVillage Ltd, (Russia)
Traffic: Global Alexa ranking of 906, with 313 million visits in the past year
Revenue Sources: Advertising, pay-per-install of potential malware, pop-unders and redirects to third-party sites, and premium accounts

This cyberlocker launched in October 2011 and has from the outset been a major source of the distribution of infringing music content. *Rapidgator* is also a major source of pre-release content, i.e., content leaked on the Internet without authorization prior to its public release date. The site offers a rewards program that shares revenue with uploaders whose material draws large volumes of traffic, thus encouraging the upload of popular copyrighted content (particularly pre-release) and undercutting any pretense that it is operating a simple cloud-based personal storage service. The Google Transparency Report reveals (as of September 2020) that Google has received delisting requests relating to over 37 million *Rapidgator* URLs. Despite the volume of infringements detected and removed from *Rapidgator*, the same content re-appears and there is no effective action being taken to prevent infringement by the service. Although it provides rights holders with a takedown account, this does nothing to prevent i) content from being disseminated (via links generated by the site) in the window *before* rights holders can intervene to take it down; ii) content which is re-uploaded after removal; and iii) content which appears in multiple locations within the site, rendering such a takedown account not a sufficiently effective solution. Users complain on social media about being ignored when trying to cancel premium accounts and cyberlocker's failure to deliver on premium services. In 2018 and 2019, on applications brought by the game and music industries, the German courts issued preliminary decisions finding the site liable for copyright infringement, and in 2019 the Russian court ordered ISPs to block access to *Rapidgator*. The corporate structure of *Rapidgator* uses a sophisticated network of offshore companies and specialized corporate vehicles to obscure the underlying beneficiaries. It is believed to be operated from Russia.

Turbobit

Domain: turbobit.net
Registrant: Uses privacy/proxy services Whois Privacy Corp., Nassau, Bahamas
Registrar: Internet.BS Corp.
Hosting Provider: Serverius Holdings, BV, The Netherlands
Traffic: Global Alexa ranking of 1282, with 327 million visits in the past year
Revenue Sources: Advertising, pay-per-install programs, paid premium accounts

Turbobit is one of the top cyberlocker sites for music piracy with nearly 360,000 infringing links identified in the past year. *Turbobit* along with *rapidgator* are two popular sites used by download sites like *newalbumreleases* to store infringing files for download. *Turbobit* derives revenue from premium accounts, advertising placed on the site, and through likely revenue-sharing arrangements with the uploaders of popular content that will attract the most traffic to the site. We believe the rewards/revenue-share arrangement is run via a separate website, *costaction.com*. *Turbobit* has been operated from the same IP address as (and is believed to be in common operation with) another cyberlocker called *hitfile* (described below). Its operators are unknown.

Chomikuj

Domain: chomikuj.pl
Registrant: Unavailable (technical contacts for the site link it to Belize and Cyprus)
Registrar: Instra Corporation Pty Ltd (Australia)
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be LeaseWeb Netherlands, B.V. (Netherlands)
Traffic: Global Alexa ranking of 8,618 with almost 125 million visits in the past year
Revenue Sources: Advertising, paid subscriptions

This site is the most popular cyberlocker in Poland. Over 80% of the visitors to *chomikuj* are in Poland, but the site hosts a broad range of U.S. repertoire. The site enables users to upload files (e.g., music, films, images, software, books) to the site and then share links to the content. Users can choose a free account or pay for an account via subscription or paid text messages. The site offers rewards to users who upload popular content downloaded by other users. The site appears to be owned and operated by a company called FS File Solutions Limited, registered in Nicosia, Cyprus. The Google Transparency Report reveals (as of September 2020) that Google has received notices to delist approximately 29 million URLs from its search results. The site has been the subject of litigation in Poland. In September 2017, the Krakow Court of Appeal held that *chomikuj* could not claim safe harbor protection because it was not "passive" and had infringed copyright.

Dbree, et al

Domain: dbree.org and related domains noted below
Registrant: Not disclosed
Registrar: Internet Domain Service, BS Corp., The Bahamas
Hosting Provider: Served through Cloudflare, (U.S.), underlying ISP believed to be Incrediserve LTD (Netherlands)
Traffic: Global Alexa ranking of 27,710, with 1.8 millions visits since emerging in April of this year; the entire network of associated sites has generated 7.4 million visits in the past year
Revenue Sources: Advertising

Dbree.org is a new locker site that appeared after *dbr.ee*, the notorious locker site used extensively by pre-release leak networks, went down. The new *dbree* is connected with a wide array of other file-hosting locker sites that demonstrate the ease with which these sites appear and disappear as content owners close in on them. In this case, the site is associated with *nippyspace.com, nippyshare.com, nippyfile.com, nippydrive.com, nippybox.com, latestmusic2018.com, xclusivejams.in, xclusivejams.net, etc*. *Dbree* is commonly found to be distributing the pre-release and newly released popular music files linked to from sites like *leakth.is*. *Dbree* and the related *nippy* sites are completely unresponsive to rights holder notifications of infringement.

Filecrypt (link protector)

Domain: filecrypt.cc
Registrant: Current Whois record shows "REDACTED FOR PRIVACY"
Registrar: Enom, Inc. (U.S.)
Hosting Provider: Virtual Systems LLC, (Ukraine)
Traffic: Global Alexa ranking of 1,595, with 141.7 million visits in past year
Revenue Sources: Banner advertisements

Filecrypt is a link protection service designed to protect links to infringing files, such as links to infringing copies of our members' music, from identification and takedown. Essentially, it acts as an encrypted, pirate linking service to infringing files. *Filecrypt* does not meaningfully apply a DMCA or copyright policy. Instead it makes a declaration on its abuse page stating that *filecrypt "does **not** host files but offers the users the possibility to provide clearly arranged hyperlinks."*

Registered users can both create containers to encrypt and share links. The "containers" can include multiple mirror links where copies of the infringing file are hosted. The ability to include mirror links is significant as it makes takedowns harder by ensuring that, where possible, the linking container will always contain one or more active links where the file can be accessed. The service is most frequently utilized by sites that engage in the distribution of pre-release leaks where rapid takedown of infringing files is most important.

Filecrypt engages in a sophisticated and targeted scheme that encourages copyright infringement by paying out to those who create and distribute links to such content via their service. The music industry has actioned over 15,500 links on *filecrypt* with only approx. 2,800 removed.

Wi.to*

Domain: wi.to
Registrant: Not publicly available
Registrar: Epag Domain Services, GMbH
Hosting Provider: BlueAngelHost Pvt. Lt (Belize)
Traffic: Global Alexa ranking of 28,235, with 10.54 million visits in the past year
Revenue: Advertising

Wi.to is a cyberlocker that has links to other well-known pre-release distribution sites and as such comprises mainly of pre-release/unreleased music. While traffic to this site is not as high as other cyberlockers, its simplicity and lightweight design, and storage of pre-release content, makes this site a clear and present danger to the global music industry. Like other cyberlockers, it generates shareable URLs to content uploaded to its servers by users and,

when those URLs are accessed, it makes those files available to download or stream via an embedded music player. The site rarely responds to notices and has only recently added an abuse address in addition to its reporting form. Anonymous uploads and downloads provide the ideal platform for illegal content to thrive.

*In the last week of October 2020, the site announced on its homepage that it was shutting down due to "legal and judicial reasons." On the surface this sounds like good news that pressure from the music copyright community was successful in shutting the site down. However, within days, a new site called *Onlyfiles.biz* emerged and appeared to have all of the same files – utilizing the same URL to access the files by simply substituting *onlyfiles.biz* for the *wi.to* in the URL. This is a prime example of the ease with which sites can migrate seamlessly between new domain names and new hosting providers. It also demonstrates the need for processes by which rights holders can readily acquire information revealing the identity of persons behind sites to achieve meaningful enforcement results.

Ddownload.com

Domain: ddownload.com
Registrant: Unlimited Networks Limited (Hong Kong)
Registrar: Namecheap, Inc (United States)
Hosting Provider: WorldStream B.V. (Netherlands)
Traffic: Global Alexa ranking of 21,901, with 24.34 million visits in the past year
Revenue: Advertising

Ddownload.com is a cyberlocker that has links to other well-known pre-release distribution sites/cyberlockers and as such comprises mainly of pre-release/unreleased music. Like other cyberlockers, it generates shareable URLs to content uploaded to its servers by users and, when those URLs are accessed, it makes those files available to download or stream via an embedded music player. Anonymous uploads and downloads provide the ideal platform for illegal content to thrive.

Anonfiles.com

Domain: *anonfiles.com*
Registrant: Privacy Protected through TuCows Inc.
Registrar: Tucows, Inc.
Hosting Provider: PROXY.IS (Proxy Provider)
Traffic: Global Alexa ranking of 6,155, with 36.08 million visits in the past year
Revenue: Advertising

Anonfiles is a cyberlocker that, as the domain name suggests, allows anonymous uploading and downloading of stored files. Like other cyberlockers, it generates shareable URLs to content uploaded to its servers by users and, when those URLs are accessed, it makes those files available to download. The site rarely responds to notices and, as such, is widely used as a storage and distribution medium for numerous pirate sites, including those distributing pre-release content. The site does not provide any method of communication other than a web form, thereby limiting our ability to escalate.

5. Unlicensed Pay-for-Download Sites

A dozen or so websites are based in Russia and the Ukraine that engage in the unlicensed sale of singles and albums at a fraction of the cost found on licensed services. The fact that they pay no royalties to copyright owners allows them to completely undercut legitimate licensed

services. The sites look professional, utilizing official album art and selling all the latest releases as well as popular older catalog works.

Mp3va

Domain: mp3va.com
Registrant: Uses privacy/proxy service MyPrivacy.net Ltd. (Canada)
Registrar: easyDNS Technologies, Inc.
Hosting Provider: Filanco LTD (Russia)
Traffic: Global Alexa ranking of 83,770, with 8.7 million visits in the past year
Revenue Sources: Sale of singles and full albums

Mp3va engages in the unlicensed sale of music. According to the site's statistics, it has over 7 million tracks and over 670,000 albums. The site has the look and feel of a legal music site like Amazon or iTunes; however, it sells single tracks for an average of 12 cents and full albums for about $1.30. Music is sold by the file size, so the cost of singles and albums varies slightly. Users must set up an account and add money to the account, using credit cards or payment intermediaries. The site also offers users two free singles upon registration to sample the website. Major U.S. payment processors have terminated support for the site, but offshore intermediaries can still be used. The site offers multiple ways for users to earn money including a 300 USD bonus after registration. The homepage provides an address for the company New Cross Network Ltd based in (Cyprus.).

Mp3fiesta

Domain: mp3fiesta.com
Registrant: Currently "Redacted for Privacy" but previously identified as Sergey Novato, Streamusic Ltd (Nicosia, Cyprus)
Registrar: Key-Systems GmbH
Hosting Provider: ASN-AVANTEL-MSK (Russia)
Traffic: Global Alexa ranking of 235,965, with 1.4 million visits in the past year
Revenue Sources: Sale of singles and full albums

Mp3fiesta operates exactly like *mp3va* in its sale of unlicensed music. Like *mp3va*, the site has the look and feel of legal music sites like Amazon or iTunes; however, it sells single tracks for an average of 15 cents and full albums for about $1.50. Music is sold by the file size, so the cost of singles and albums varies slightly. The site notes its prices are less than top-5 digital music retailers and boasts having over 4.2 million tracks and over 390,000 albums available. The site offers selected special deals for some music, such as a 20% discount on artist content on the artist's birthday. Like on *mp3va*, *mp3fiesta* users must set up an account and add money to the account, using credit cards or payment intermediaries, and then purchases are made drawing down from funds available in the account. The contact page on the site provides details for a company called Tokovina Holdings Ltd, based in (Cyprus).

6. Additional Issues

Piracy within Mobile Apps

Telegram App: Telegram is an instant messaging service which allows users to communicate via text and voice message. On its face, the app might appear to be of no

special concern. However, Telegram users are able to create channels which allow the operator of the channel to distribute messages and content to all members of the channel. Often channels include scripts known as bots which provide some level of interactivity within the channel, sometimes allowing users to request specific content from the channel. Telegram offers many user-created channels which are dedicated to the unauthorized distribution of copyrighted recordings, with some channels focused on particular genres or artists. Telegram itself hosts many of the copyrighted recordings made available through these channels and the RIAA has sent DMCA notices to Telegram containing over 18,000 instances of copyrighted recordings offered without authorization through these channels.

Telegram claims that it forwards our notices to the channel operators who are responsible for removing the infringements listed in our notices. We have found, however, that most channel operators appear to take no action in response to our notices, with nearly all of infringements listed in our notices remaining available. Likewise, Telegram makes no apparent attempt to verify that channel operators have complied with our notices and does not seem to have any kind of repeat infringement policy. Telegram is accessible through various client applications, including popular mobile apps available through the Apple App Store and Google Play.

Bulletproof ISPs

As noted above, infringing sites are turning more towards offshore hosting ISPs that support the sites' infringing activities. These "Bulletproof" ISPs support various types of criminality through considerable leniency in the kinds of materials they permit to be uploaded and distributed via their networks. These ISPs do not respond to notices of infringement or warning letters that the ISP is hosting and supporting known infringing sites. The two most problematic bulletproof ISPs that support infringing activity relating to music are:

- **Ecatel/Quasi Networks (Novogara LTD and Incrediserve LTD) – Seychelles / Amsterdam.** Ecatel is a Dutch hosting provider founded in 2005, registered in the UK, and headquartered in The Hague. It offers offshore hosting options and, over the last decade, has consistently hosted criminal and toxic content, and generated spam and DDoS traffic from its IP space. Ecatel is known to law enforcement, has been shut down by its peers at least once (in 2008), and was subject in 2012 to DDoS attacks by Anonymous for hosting child pornography. In 2017, BREIN raised an action against Ecatel and its associated hosting companies for the hosting of, and failure to remove, infringing and illegal content. One such associated hosting company is Quasi Networks (http://www.quasinetworks.com/) operated from Mahe, Seychelles with the infrastructure located in the Netherlands. Quasi Networks is or has been in the past responsible for hosting various sites engaged in the transmission of pre-release works, including *dbree.org*, and the series of "*nippy" prefixed locker sites*, *xclusivejams*, *mp3monkey.net*, *gosongs*, and *leakth.is*. With little recourse to remove infringements, both Ecatel and Quasi represent a significant danger to our member companies.

- **FlokiNET – Romania/Iceland/Finland.** FlokiNET (https://flokinet.is/) is a web hosting service that prides itself on allowing the completely anonymous hosting of content across its three server locations: Romania, Iceland, and Finland. In a recent

case involving pre-release music piracy for a site known as *musicmafia.to*, FlokiNET was listed as the registrant of the domain. FlokiNET advertises quite openly, "We do not require any personal details or identification; any valid e-mail address is enough information to be a client." As a result, many different types of websites hosted on the ISP host bestiality pornography and fraudulent sites, amongst others. Other infringing sites that have been hosted on FlokiNet include *avxhome.se*, *djnotorioussam.com*, and *x1337.to*. The operator of FlokiNET is known to the authorities and resides in Romania but, to date, no action has been taken to close the service.

Nigerian-Operated Infringing Sites

We have continued to see a significant growth in the number of Nigerian-operated sites that are distributing direct download links for pre-release and newly released music affecting our member companies. The number of such infringing sites with a Nigerian operator stands at over 400. These sites are a great cause for concern to the industry as they generally disregard infringement notices and refuse to disable access to content. They are particularly damaging as they prevent the growth of legitimate services in emerging markets. The sites' primary method of promotion is via Twitter, and most sites make use of the Nigerian-operated ISP speedhost247.com.

Intermediaries

Reverse Proxy Services to Obfuscate Hosting ISP. These services are utilized by pirate websites to hide the identity and location of actual hosting ISPs. More and more pirate sites employ reverse proxy services, most commonly Cloudflare, to obfuscate their IP address, creating obstacles to enforcement against such sites. While Cloudflare will provide the underlying IP address upon request when presented with an infringing URL, Cloudflare also notifies its customer of the request, whereby the customer can quickly migrate its site to a new hosting ISP while continuing to utilize Cloudflare. Since there is no real-time access to the site's location, any IP address provided by Cloudflare one day may be inaccurate the next. In October 2020, Cloudflare was ordered by a Court in Germany to block access to infringing content available via its customer's website or block the entire website. This was the first time a German Higher Regional Court has confirmed a preliminary injunction against an anonymization service and thus prohibiting third parties from disseminating illegal offers while concealing the identity of the servers of structurally infringing websites. A more recent trend is the growth and use of alternative reverse proxy services by site operators consumers such as Succuri (GoDaddy, Inc) and DDOS-Protection.ru (Russia).

Njal.la Registrar. Njal.la purports to be a registrar when in reality it operates more as a domain name buyer and a privacy service provider. The service purchases a domain name on the client's behalf and allows the client to control the administration of the domain without being the legal owner. Its website states that "*We're not going to give your customer data out easily*". While its website lists "health and safety" as one of the reasons that they might give out customer information, copyright or the violation of the rights of others is not listed. Many copyright infringing services are using this service to prevent right holders from identifying the operators of pirate sites. In fact, the service openly advertises on its website that some of its operators "have also been involved in projects like The Pirate Bay and Piratbyrån to mention a few things. Or to keep it simple; we've got a long history and serious understanding of the issues of anonymity on the internets" (sic). The service is

run by 1337 LLC based in Nevis in the Caribbean and was established by Peter Sunde (one of the co-founders of The Pirate Bay). Furthermore, 1337 LLC shares its name with 1337x.to which is a notorious torrent index website also listed in this submission.

.to ccTLD Registry. TONIC, Inc (San Francisco, United States), manages the .to ccTLD registry on behalf of the Kingdom of Tonga. The registry does not provide any WHOIS information publicly or on request, other than the nameserver information. Infringing websites that engage in music piracy continue to use the .to ccTLD to hide their identities and operations, including those listed in this submission. Over the years, we have identified over 80 pirate sites operating from the .to TLD. The most pressing ones today are those associate with hacked and leaked recordings. TONIC, Inc, the US company that administers the .to TLD, has refused to remove infringing websites despite evidence of serious infringement and criminal activity being demonstrated.

PHYSICAL MARKETS

In 2018, physical CD and vinyl album sales continued to generate considerable revenue for U.S. record companies. Prominent ecommerce platforms have become the ideal outlet for counterfeit physical products being produced in Russia and China. In some cases, Russian and Chinese sellers will sell directly on retail platforms, shipping the goods to consumers from Russia or China. In other cases, the principals behind the Chinese and Russian counterfeits sell to third-party sellers on platforms that may or may not know they are buying and reselling counterfeits.

Chinese and Russian Counterfeit CD Manufacturing and Distribution

Counterfeit CDs and vinyl albums being manufactured and sold out of China and Russia are high quality products made to closely resemble authentic ones. These counterfeits can be readily identified by our experts even though the tell-tale signs of counterfeits are not apparent to casual observers. The outside packaging will copy pull tabs, security seals, and shrink-wrap, while the insert booklets will mirror the legitimate versions of the product, printed on high-grade commercial printing machinery. In addition to straight-up counterfeit copies of legitimate album releases, we have also seen a rise in the manufacture of compilation “Best of” and “Greatest Hits” albums that were never released by the record labels. With the rise in popularity of vinyl albums generally, we are finding the unauthorized manufacture and sale of vinyl versions of albums that were only officially released digitally or in CD format. Finally, we are finding counterfeit versions of official box sets discographies as well as unauthorized pirate box sets discographies.

Test purchases, surveys, and enforcement programs have established that massive quantities of these counterfeits were finding their way into the legitimate market principally through various ecommerce platforms like Amazon, eBay, and AliExpress. Consumers are paying full price for counterfeit offerings appearing alongside legitimate offerings, resulting in one-for-one displacements of legitimate sales.

An essential element for these platforms in protecting their customers and copyright owners from these Chinese and Russian counterfeits lies first and foremost in pre-screening sellers to ensure they have legitimate sources of supply. Amazon has initiated such a program, but the

other major platforms have not. Each of these platforms has established processes by which counterfeit offerings can be reported and removed; however, there appears to be inconsistent action against repeat infringers. In addition, titles identified as infringing because there is no legal version of the title (e.g., "greatest hits," vinyl albums) are not being removed from platforms across the board. More can be done by ecommerce platforms to prevent counterfeit products illegally manufactured and sold from Russia and China from infiltrating the legitimate marketplace here and around the world.

ISSUE FOCUS – ECOMMERCE PLATFORMS AND OTHER THIRD-PARTY INTERMEDIARIES

The issue focus for the 2020 Notorious Markets List will examine the use of ecommerce platforms and other third-party intermediaries to facilitate the importation of counterfeit and pirated goods into the United States.

As described above, most of the physical counterfeit and pirate music products are being manufactured in Russia and China. These products are finding their way into the U.S. and European markets through ecommerce platforms, principally eBay, Amazon, and Shopify-supported websites. Test purchases, surveys, and enforcement efforts have established that massive quantities of these counterfeit and pirate products are being made available on these platforms. Consumers are paying full price for counterfeit offerings appearing alongside legitimate offerings, resulting in a one-for-one displacement of a legitimate sale.

An essential element for these platforms in protecting their customers and copyright owners from these Chinese and Russian counterfeits lies first and foremost in pre-screening sellers. AliExpress has addressed the problem by simply not authorizing the sale of CDs and other music formats on their platform. Periodically these products will appear under different categories, and without CD or album descriptions, so they are difficult to find. When they are discovered, sellers and counterfeit offerings are promptly removed. Amazon has likewise initiated programs to fight counterfeits being sold on its platform. When widespread problems were brought to their attention several years ago, Amazon took steps to restrict accounts to sellers who could establish legitimate commercial sources for products. The result has been a substantial reduction in the amount of counterfeit or pirate offerings on Amazon.

As these platforms have taken steps to weed out sellers of counterfeit products, sellers have migrated to other platforms. Today we see eBay as the ecommerce platform where Russian and Chinese counterfeit products are being widely sold. While eBay has established effective processes whereby counterfeit offerings can be removed, there appears to be inconsistent action against repeat infringers. In addition, titles identified as infringing because there is no legal version of the title (e.g., "greatest hits," vinyl albums) are not being removed from the platform across the board. eBay still remains our biggest source of infringing CDs, box sets, vinyl albums, and face masks. Despite regular calls and meetings with eBay over the years, it continues to be the platform with the most amount of infringing products available for purchase. We have seen very little proactive work on their part to implement any seller vetting so we have seen pirate sellers operating under multiple accounts under different names so that if one account is terminated the sellers can immediately shift the counterfeit offering to a different seller account.

* * *

We hope you find this information useful, and we look forward to continuing to work with the U.S. government to find solutions to these problems.