January 2023

Corsearch calls for Cloudflare to do more

TO PROTECT CONSUMERS & IP OWNERS.

Simon Baggs, President, Brand & Content Protection

Mike Sweeney, Director and Senior Legal Counsel

Joseph Cherayath, Vice President, Enforcement

Naiara P. Cunha, Director, Brand Protection – EMEA

CORSEARCH®

Table of Contents

Executive Summary

Many of the websites that Corsearch identifies as engaged in brand and content infringement use Cloudflare's services (71% of all websites notified by Corsearch and demoted by Google[1], 49% of all websites enforced by Corsearch for content piracy and 23.5% of all websites enforced by Corsearch for counterfeiting)[2].

These websites are not hosted by Cloudflare and Cloudflare maintains that it is not responsible for moderating the content of websites that use its services. There have been several litigation cases to determine the extent of Cloudflare's liability. Regardless of liability, many Internet intermediaries have agreed to take steps to prevent harm to consumers where operators are using their services to infringe intellectual property.

This paper explains the enforcement data Corsearch has concerning Cloudflare and invites Cloudflare to take specific actions to help prevent the misuse of Cloudflare's services by those operating counterfeit and pirate websites.

We urge Cloudflare to stop providing services to infringing websites that put consumers at risk.

> 71% of all websites notified by Corsearch and demoted by Google use Cloudflare.

> 49% of all websites enforced by Corsearch for content piracy use Cloudflare.

> 23.5% of all websites enforced by Corsearch for counterfeiting use Cloudflare.

Stopping piracy & counterfeiting

Cloudflare should act to protect consumers and IP owners and cease providing services to pirate or counterfeit websites without requiring a court order when they are notified as follows:

Piracy Websites

- where Google has already taken action against a particular website; and/or
- where a website has been determined as infringing IP by a court and/or is engaged in criminality (as determined by a recognized law enforcement body or international organization with similar standing concerning IP infringement).

Counterfeit Selling Websites

- Where a website is selling counterfeit goods and using a domain name which copies the brand name for the products. Google will remove the website from its search results. Cloudflare should mirror this policy; and
- Where a website is selling counterfeit goods but not using the brand name in the domain name, Cloudflare should withdraw services where it is clear that the website is substantially dedicated to counterfeiting and serves no legitimate purpose.

Introduction & Background

Corsearch finds and removes brand infringements and pirate content from Internet locations such as online marketplaces, social media platforms and stand-alone websites. Corsearch works with hundreds of brands and content creators to stop IP infringement online to protect consumer trust. Each year, Corsearch's technology reviews billions of potential infringements and secures the removal of hundreds of millions of counterfeit products and pirate content.

The proliferation of unlawful products, services and content online undermines consumer trust and can lead to substantial consumer harm. The unwitting online purchase of a counterfeit pharmaceutical can have lethal consequences. The download of a pirate movie can infect hardware with viruses and malware. In either case, the persons behind the sale of counterfeit products and the distribution of pirate content may be involved in organised criminal activity[3].

Cloudflare is a business based in San Francisco which operates in over 25 countries and is listed on the New York Stock Exchange. Cloudflare provides services to millions of legitimate websites and businesses[4] to enhance their performance and end-user experience and to mitigate cyberattacks. One of the services that Cloudflare provides is its Content Delivery Network (see below).

Cloudflare provides a range of services to people and organizations operating websites on the Internet. Many of these services are valuable. In particular, Cloudflare helps businesses and individuals to avoid cyberattacks (including through blocking Denial of Service attacks) and also to enhance website performance.

Cloudflare's total forecasted revenue for FY2022 is $970m (its second quarter revenue increasing by 54% Y-O-Y)[5].

Cloudflare's services include the provision of Content Delivery Network ("CDN") services through a geographically distributed network of servers. CDNs provide high levels of availability and performance by reducing load on servers and distributing services spatially relative to end-users. CDN services alleviate performance "bottlenecks" on the Internet and speed up the delivery of content to end users.

Cloudflare has sometimes disputed that its services increase speed of delivery. Cloudflare was invited to comment on this paper. At the date of publication, Corsearch is yet to receive a response.

> The unwitting online purchase of a counterfeit pharmaceutical can have lethal consequences. The download of a pirate movie can infect hardware with viruses and malware.

To protect consumer trust by reducing the availability of IP infringing content and products, Corsearch uses technology to find infringements and send notices to online operators (such as marketplace platforms, social media sites and website operators) with enough detail to make these operators liable for infringement if they refuse to take action. For example, if Amazon is used to offer a counterfeit product for sale, it is a host of that offer and Corsearch will send a notice to it. If Amazon subsequently fails to remove the product, Amazon may be liable for the infringement. The structure for host liability in the online context is set by legislation[6].

The ability for a rights owner to notify a host is a key part of enforcement strategy in the online context. Without this, a rights owner would be required to pursue each individual person who is responsible for uploading infringing content to the Internet or for operating a particular website or marketplace store that offers fake products for sale. Often the person originally responsible for uploading infringing content or for offering a counterfeit product is not clear. In the case of websites, often the operator of an infringing website will not register his or her genuine name when registering the site and he or she will do everything possible to remain anonymous. If it were necessary to be certain of the identity of every seller or uploader, protection of IP online would be almost impossible.

Whilst Cloudflare also provides conventional hosting services, the issue here concerns its CDN services and that is the subject of this paper.

Where Cloudflare's CDN services are used by a website, the actual host for the website is not revealed. This means that from an enforcement perspective, when a website infringes IP and uses Cloudflare as its CDN provider, the only information immediately available to the rights owner is that Cloudflare is providing CDN services. The operator of the site is not revealed and nor is the true host location for the site.

When a website infringes IP and uses Cloudflare as its CDN provider, the only information immediately available to the rights owner is that Cloudflare is providing CDN services. The operator of the site is not revealed and nor is the true host location for the site.

Why use Cloudflare's Services

Unlike its competitors, Cloudflare offers sophisticated technology services to its customers (including Denial of Service protection and SSL certification services among others) free of charge. Those services are typically offered by Cloudflare's competitors as premium, paid-for services.

Alternative CDN providers are also known to have much more stringent practices when they are notified about infringement, typically requiring that infringing material is removed by a host promptly, failing which CDN services may be terminated.

In addition, Cloudflare does not require its customers to provide verified identification and business or personal registration details, essentially granting them a cloak of anonymity under which to operate. The incentive for bad actors to contract with Cloudflare for services is therefore plain to see.

In 2016, the Recording Industry Association of America ("RIAA"), a trade association which represents the recorded music industry in the United States, made submissions to the United States Trade Representative (the "USTR") in which it highlighted the "thousands of websites on the internet" which are dedicated to music piracy. In highlighting some examples which "create the most damage to the US recording industry" the RIAA emphasised that Cloudflare's services were in many cases being used to "obfuscate" the hosting provider. In 2019, the RIAA , the Motion Picture Association (the "MPA") and the Association of American Publishers submitted to the USTR that Cloudflare was frustrating enforcement efforts by helping pirate sites to hide their hosting locations. In addition, the Hollywood-affiliated Digital Citizens Alliance noted that "Cloudflare's services popped up the most in [its] latest review of companies supporting content theft websites that expose consumers to malware".

> Cloudflare does not require its customers to provide verified identification and business or personal registration details, essentially granting them a cloak of anonymity under which to operate.

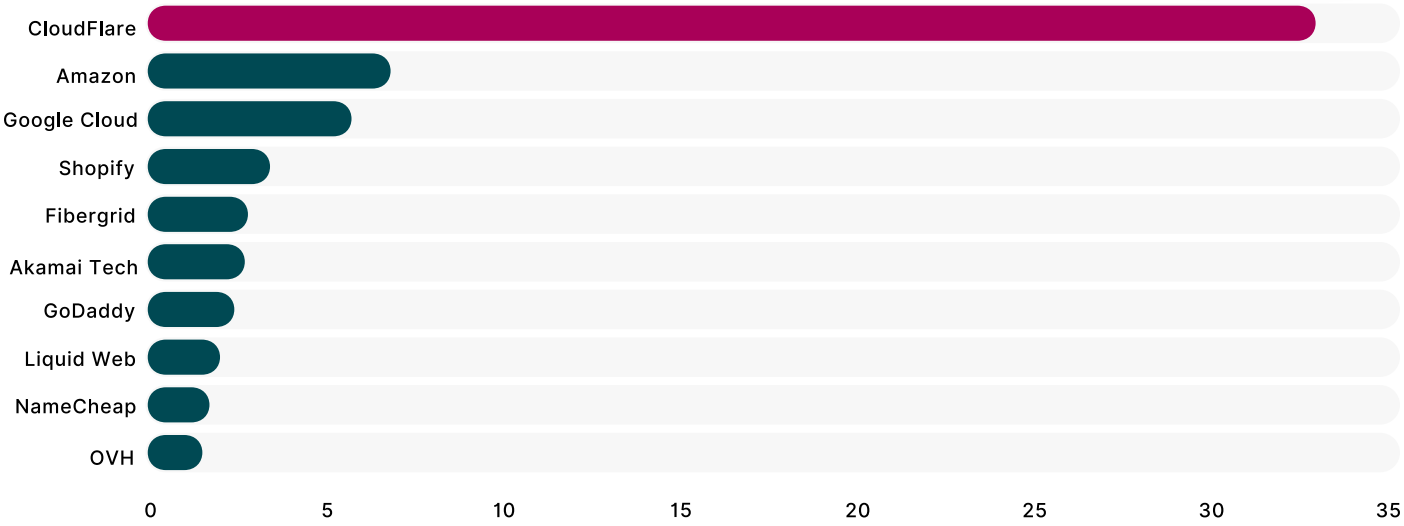
Cloudflare issued a rebuttal, commenting that the complaints were "misleading". The rebuttal goes on to say that Cloudflare "does not host the referenced sites, cannot block websites and is not in the business of hiding companies that host illegal content".

More recently (October 2022), the MPA filed a submission on behalf of its member studios (which were stated to include Netflix, Walt Disney Studios, Paramount Pictures, Sony Pictures, Universal Studios and Warner Bros, Entertainment) to the USTR. In that submission, the MPA commented that "Cloudflare's customers include some of the most notorious, longstanding pirate websites in the world, including the massively popular streaming site cuevana3.me and The Pirate Bay, whose current domain, thepiratebay.org, has been identified as infringing rights holders' copyrights nearly six million separate times".

The International Federation of the Phonographic Industry (a trade association which represents the recorded music industry globally) has also made similar submissions to the European Commission's Counterfeit and Piracy Watchlist

Corsearch Data Intelligence

Overall Percentage: Enforced Websites [FIG1]



Corsearch has analysed its data to identify the websites that its technology detected as engaged in the infringement of trademarks and copyright during 2021. In most cases, where the websites detected were not using Cloudflare, the provider of hosting services was known. In cases where the websites were using Cloudflare's services, the host provider was not detected by Corsearch because Cloudflare's services do not reveal the host.

Figure 1.

Figure 1 considers the intermediaries identified most often by Corsearch relating to websites that have infringed trademarks or copyright. In most cases, the intermediary is the host because the host is readily identifiable. In cases where the website is using Cloudflare, the host is not identifiable without further investigation and so the intermediary mostly closely associated with these websites is Cloudflare. The top ten intermediaries support 60.4% of all of the websites enforced by Corsearch.

32.6% of all of the websites enforced by Corsearch use Cloudflare's services.

Figure 2 shows the top ten intermediaries associated with websites enforced by Corsearch in respect of trademark infringement. The nine providers other than Cloudflare are hosting providers. Cloudflare is not the host of these websites. However, the host is not readily identifiable and Cloudflare is most closely associated with them.

Brand Protection: Percentage of Enforced Websites. [FIG2]

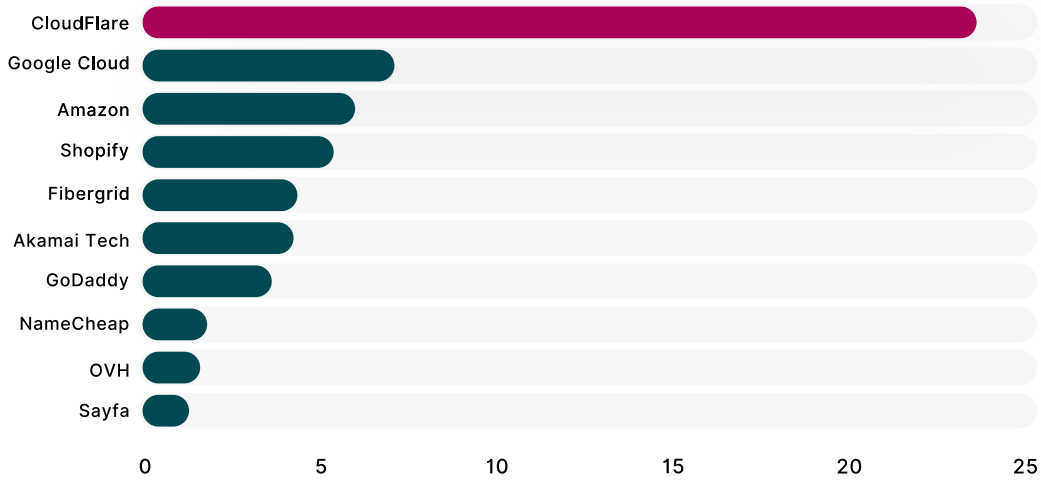


Figure 2.

Figure 3 shows the top ten intermediaries associated with websites where URLs on those websites have been notified for search engine delisting by Corsearch in respect of copyright infringement. The nine providers other than Cloudflare are hosting providers. Cloudflare is not the host of these websites. However, the host is not readily identifiable and Cloudflare is most closely associated with 49% of websites notified for delisting by Corsearch.

Content Protection: Delisting: Percentage of Websites. [FIG3]

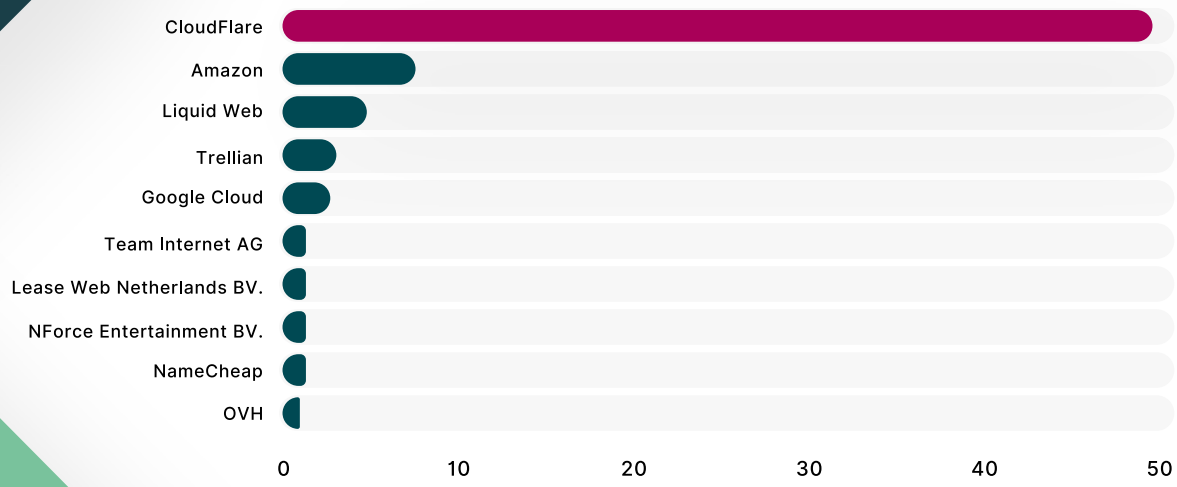


Figure 3.

Cloudflare's Approach to Notices sent on behalf of Rights Holders

At present, when Cloudflare is notified about a website using its services, it will reveal to the rights owner the hosting provider of the website, its IP address and an "abuse contact" email address where one has been provided.

The text below is an extract from Cloudflare's website:

"When rightsholders find infringing content on websites using [our] services, they sometimes contact Cloudflare because our IP addresses and nameservers appear in the place of the websites' hosting providers. Although we are unable to remove content from the Internet that we do not host, we are able to connect rightsholders with the website operators and hosting providers who can. We forward copyright complaints to website operators and hosting providers, and give rightsholders the hosting providers' contact information. While we are not legally obligated to provide that sort of assistance, we think it is the right thing to do and the best way for us to help[15] ".

The Cloudflare Website contains a section where users can report abuse under various headings including DMCA complaints, Phishing, Trademark infringement and others

The Cloudflare Reporting Form displays the following, prominent notice:

"Cloudflare doesn't host web content and cannot remove content from a website. Cloudflare complies with valid copyright complaints when receiving complaint proof from the copyright holder or authorized agent for the copyright holder. When presented with a valid complaint, Cloudflare provides information about the web hosting provider."

When an enforcement notice is issued to Cloudflare, it will notify its "customer" of the report and will forward the report "on to the responsible hosting provider".

Cloudflare Can Do More to Protect Brand & Content Owners

Cloudflare is uniquely positioned to do more to protect rights holders and substantially to suppress the scourge of online piracy and counterfeiting

As Figure 1 shows, Cloudflare is a key intermediary whose services are fundamental to the operation of websites which infringe intellectual property and cause damage to brand and content owners. There is no doubt that if Cloudflare was prepared do more to assist rights owners, the landscape would be substantially improved for rights owners, given the propensity among bad actors to contract with it for services for the reasons outline above (no cost to the website operator coupled with lack of KYC and anonymity). If Cloudflare's policies were more stringent, fewer bad actors would use its services.

We are asking Cloudflare to do more to support rights owners by voluntarily implementing certain measures. These measures are reasonable, proportionate and if adopted by Cloudflare will have a significant impact.

Corsearch requests of Cloudflare

Request 1.

Cloudflare should take action where Google has removed or demoted a URL. Where Corsearch confirms to Cloudflare that Google has deindexed or demoted a website, Cloudflare should terminate services to all current and future domains for that website.

Request 2.

Cloudflare should withdraw services to any website which has been accepted by a recognised law enforcement body as being unlawful and in particular where the website appears on the IWL (and where Cloudflare is providing services to it).

Request 3.

Where Cloudflare is providing services to a standalone infringing website, recognised by the USTR for inclusion on the NML, Cloudflare should stop providing services to that website.

Request 4.

Where Cloudflare is providing services to a standalone infringing website, recognised by the Counterfeit and Piracy Watchlist, Cloudflare should stop providing services to that website.

Request 5.

We are asking Cloudflare to mirror Google's approach and withdraw services to websites notified to it (supported by accompanying documents including registered trademark certificates) on the grounds that the website offers for sale counterfeits and is operated under a domain name which incorporates a registered trademark.

Request 6.

Cloudflare should withdraw services to websites:

(i) when Corsearch notifies Google about a URL which infringes trademarks by selling counterfeits, we will also notify the same URL to Cloudflare (where that website is enabled by Cloudflare); and

(ii) where it is clear that the website is substantially dedicated to counterfeiting and serves no legitimate purpose.

Request 7.

Cloudflare should publish a comprehensive transparency report containing, amongst other things, the domain name for the websites using its services which have been reported by rights holders.

Request 8.

Cloudflare should implement "Know-Your-Client" procedures which (as a minimum) should include the provision of information including, but not limited to, verified, formal identification documents (in the form of government ID or business registration documents), bank account registration details and verified telephone and email information. Where the information is not provided, Cloudflare should not provide services. Without these requirements, bad actors will continue to contract with Cloudflare, safe in the knowledge that they can provide false or incomplete information.

Websites which Infringe Copyright ("Piracy Sites")

Search Engine Data

Google is required by legislation to remove search results from its main index where rights owners (or their agents) notify it of infringing URLs. Where a threshold is met (in terms of the number of reported URLS) Corsearch's experience is that Google will either demote the website or remove it from its index altogether. Google undertakes this demotion recognising that the website is fundamentally unlawful where a large number of notifications have been sent to it in relation to the same website. Corsearch maintains a dataset of websites it has reported to Google for deindexing. Upon reaching a threshold (in terms of number of infringing URLs), Google is prepared to accept that the website in question is unlawful and will demote it. Corsearch has done extensive analysis around these demoted websites and has established that more than 70% use Cloudflare's services.

We are asking Cloudflare to take action where Google has removed or demoted a URL. Where Corsearch confirms to Cloudflare that Google has deindexed or demoted a website, Cloudflare should terminate services to all current and future domains for that website.

This approach ensures that Cloudflare is not being asked to evaluate whether a website is concerned in unlawful piracy (or not). Instead, Cloudflare is presented with a quantitative approach which establishes a threshold, above which Cloudflare should intervene and withdraw its services.

We are asking Cloudflare to take action where Google has removed or demoted a URL. Where Corsearch confirms to Cloudflare that Google has deindexed or demoted a website, Cloudflare should terminate services to all current and future domains for that website.

Law Enforcement Data and Governmental Organisations

The Police Intellectual Property Crime Unit ("PIPCU") is a department of the City of London Police, the national lead force for fraud. It was established in 2013 with the responsibility to investigate and deter serious and organised intellectual property crime in the United Kingdom.

Part of PIPCU's remit is to protect consumers from harm, focusing on intellectual property crime that has public safety implications. Since its inception, it has investigated intellectual property crime worth more than £100 million concerning counterfeit goods or digital piracy and suspended more than 30,000 websites selling counterfeit goods. These websites have also been linked to identity theft.

PIPCU launched Operation Creative and the Infringing Website List (the "IWL") in 2013 to tackle the funding of illegal streaming websites that adversely impact the UK's creative industries. This is a police endorsed list of websites which host copyright infringing content. It is used by advertisers and advertising networks to ensure that their adverts do not appear on these websites and that revenue is not handed to their operators.

Corsearch analysed all of the websites that are currently active on the IWL list. The result was that 67% of those websites uses Cloudflare's services.

Websites which have been placed on the IWL have been determined by PIPCU to be unlawful. We are therefore asking Cloudflare to withdraw services to any website which has been accepted by a recognised law enforcement body as being unlawful and in particular where the website appears on the IWL (and where Cloudflare is providing services to it).

The Notorious Markets List (the "NML") is a report published every year by the United States Government (the Office of the United States Trade Representative (the "USTR")). It highlights online and physical markets (and other internet locations including websites) operating outside of the United States, which reportedly engage in or facilitate substantial trademark infringement and copyright piracy. Rights owners and trade associations are consulted and are encouraged to provide feedback each year prior to publication. As such, it is an influential and persuasive document which seeks to educate and inform rights holders and consumers around counterfeiting and piracy.

Where Cloudflare is providing services to a standalone infringing website, recognised by the USTR for inclusion on the NML, Cloudflare should stop providing services to that website.

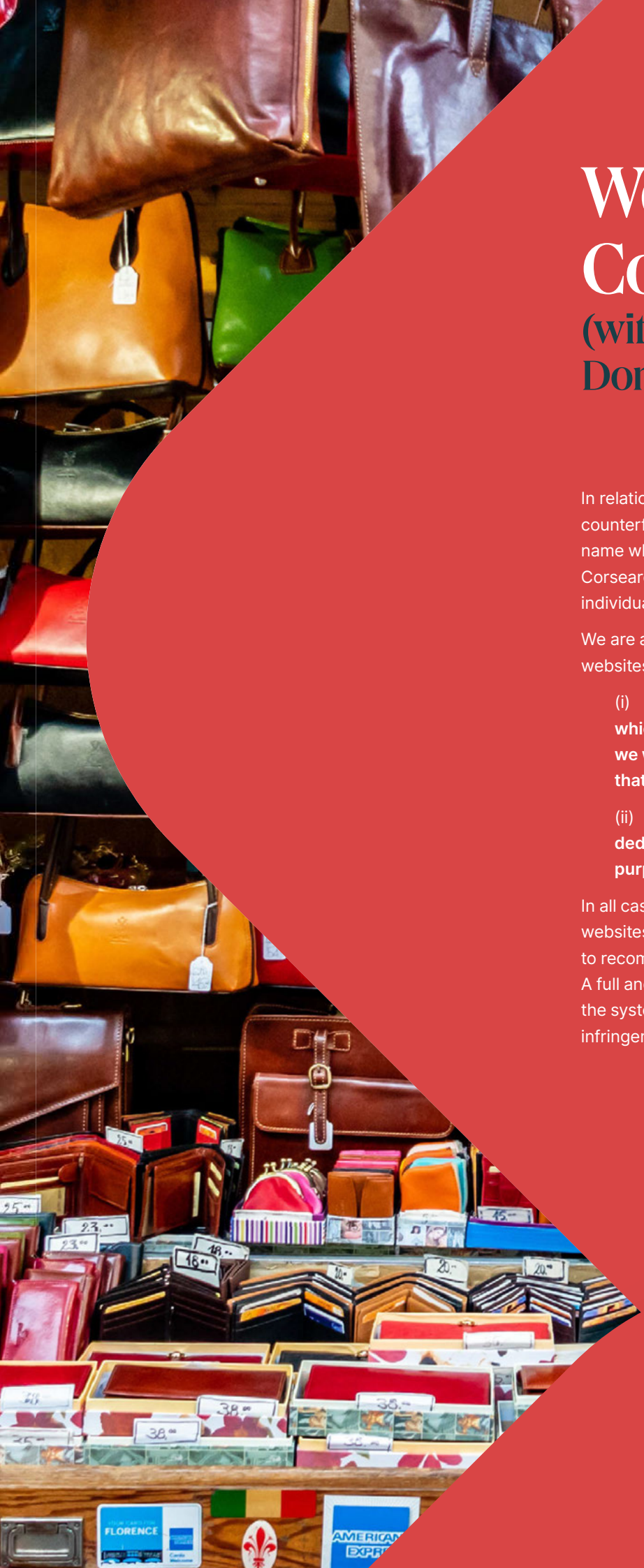
The Counterfeit and Piracy Watchlist is a similar document published each year by the European Commission. In 2018, the report noted that, according to the creative industries (film, music, book publishers, etc.) and other organisations, Cloudflare is used by approximately 40% of the pirate websites in the world [16]. **Again, where Cloudflare is providing services to a standalone infringing website, recognised by the Counterfeit and Piracy Watchlist, Cloudflare should stop providing services to that website.**

Websites Selling Counterfeits

(with the use of Infringing Domain Names)

In relation to websites which are concerned in the sale of counterfeit goods and which are operated under a domain name which incorporates a proprietary trademark, Corsearch's experience is that Google will remove websites notified to it.

We are asking Cloudflare to mirror this approach and withdraw services to websites notified to it (supported by accompanying documents including registered trademark certificates) on the same grounds (i.e the website offers for sale counterfeits and is operated under a domain name which incorporates a registered trademark).



Websites Selling Counterfeits
(without an Infringing Domain Name)

In relation to websites which are concerned in the sale of counterfeit goods (but which are operated under a domain name which does not incorporate a proprietary trademark), Corsearch's experience is that Google will remove individual URLs from its search results, upon being notified.

We are asking Cloudflare to withdraw services to those websites under the following circumstances:

(i) **when Corsearch notifies Google about a URL which infringes trademarks by selling counterfeits, we will also notify the same URL to Cloudflare (where that website is enabled by Cloudflare); and**

(ii) **where it is clear that the website is substantially dedicated to counterfeiting and serves no legitimate purpose.**

In all cases where Cloudflare withdraws services to websites under these proposals, it would of course be free to recommence services if the websites stop illegal activity. A full and long term ban may be required if websites game the system by repeatedly stopping and then restarting infringement.

Cloudflare Transparency Report

Complaints notified to Google are published and made available through the Lumen database[17] within the Google Transparency Report. The Lumen database "collects and analyses legal complaints and requests removal of online material, helping Internet users to know their rights and understand the law. This data enables [Lumen] to study the prevalence of legal threats and let Internet users see the source of content removals".

As noted above, Cloudflare is a major player in the intermediary ecosystem for websites that infringe copyright and trademarks. Given the extent to which its services are misused by website operators, there is understandable concern across the industry to ascertain the volume (and nature) of complaints notified to Cloudflare.

Cloudflare should therefore publish a comprehensive transparency report containing, amongst other things, the domain name for the websites using its services which have been reported by rights holders.

Cloudflare should publish a comprehensive transparency report containing, amongst other things, the domain name for the websites using its services which have been reported by rights holders.

Know Your Client

The lack of verifiable information around who the parties are behind the operation of a website substantially impedes rights holders from the point of view of beginning an investigation and/or enforcement. This issue would be easily resolved if Cloudflare implemented "Know-Your-Client" procedures which (as a minimum) should include the provision of information including but not limited to verified, formal identification documents (in the form of government ID or business registration documents), bank account registration details and verified telephone and email information. Where the information is not provided, Cloudflare should not provide services. Without these requirements, bad actors will continue to contract with Cloudflare safe in the knowledge that they can provide false or incomplete information.

Conclusion

As the data and analysis in this paper makes clear, many infringing websites use Cloudflare's services. The landscape for rights owners seeking to prevent infringement of their IP on websites would be substantially improved if Cloudflare was prepared to amend its policies in line with the suggestions in this paper. Our suggestions are reasonable and capable of implementation with relative ease. We urge Cloudflare to engage with Corsearch to agree a process for notification to them and response by them that will help ensure consumer trust is protected.

© Corsearch, Inc.
and/or its affiliated companies.
All rights reserved.

Source Index

1. Note that Figure 3 covers both notification for delisting by search engines and others. Where sufficient notices are sent to Google, sites can be demoted. 71% of the sites notified by Corsearch that have been demoted by Google use Cloudflare's services.
2. See for further detail (pages 6-8)
3. https://www.europol.europa.eu/media-press/newsroom/news/europol-%E2%80%93-eu-ipo-report-ip-crime-and-its-links-to-other-serious-crimes
4. https://trends.builtwith.com/cdn/Cloudflare
5. https://cloudflare.net/news/news-details/2022/Cloudflare-Announces-Second-Quarter-2022-Financial-Results/default.aspx#:~:text=For%20the%20full%20year%20fiscal,outstanding%20of%20approximately%20343%20million
6. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the "Ecommerce Directive") (Article 14) and the Digital Millenium Copyright Act 1998 (https://www.copyright.gov/legislation/dmca.pdf)
7. https://www.regulations.gov/comment/USTR-2016-0013-0012
8. https://www.regulations.gov/comment/USTR-2019-0013-0010
9. https://www.regulations.gov/comment/USTR-2019-0013-0011
10. https://www.regulations.gov/comment/USTR-2019-0013-0007
11. https://www.regulations.gov/comment/USTR-2019-0013-0002
12. https://www.regulations.gov/comment/USTR-2019-0013-0025
13. https://www.regulations.gov/comment/USTR-2022-0010-0022
14. https://circabc.europa.eu/ui/group/e9d50ad8-e41f-4379-839a-fdfe08f0aa96/library/bc70024a-4b65-44cb-a383-3c22a094bc24/details
15. https://support.cloudflare.com/hc/en-us/articles/360028158352-Reporting-abuse-to-Cloudflare#h_0981c0c6-faef-4612-96e1-a351095c82b3) (the "Cloudflare Reporting Form").
16. https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf
17. https://lumendatabase.org/

CORSEARCH®