

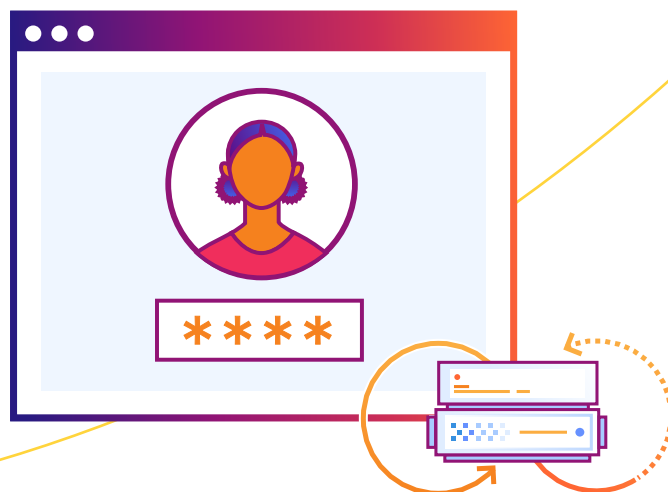
H2 2024 – Abuse Processes

Cloudflare Transparency Report



Abuse Processes

An essential part of earning and maintaining the trust of our customers is being transparent about the actions we take in response to reports of abuse and legal orders to address content on websites using our services. To this end, and consistent with the transparency reporting obligations under the European Union's (EU) Digital Services Act (DSA), Cloudflare publishes semi-annual updates to our Transparency Report regarding our service-specific abuse processes. We list on our [Transparency Center](#) some things that Cloudflare has never done and would resist through all available legal remedies in order to protect our customers from illegal or unconstitutional requests. More details regarding how Cloudflare addresses the abuse issues described in this report can be found in our [Trust Hub](#).



Content

4	Our Guiding Principles
5	Background on Content Removal and Blocking
6	The Data
	Actions Taken on Hosted Content
	Hosted Abuse Processes
	Non-Hosted Restrictions of Access
	Orders Relating to Pass-Through Services
	Mitigation of Phishing and Technical Abuse on Non-Hosted Services
	Requests for Content Blocking Through DNS Resolver
	Termination or Suspension of Services
	U.S. Court Orders
	Uniform Domain-Name Dispute Resolution
	Termination of Services Due to CSAM
	Voluntary Terminations
	Third-Party Reporting
	Reports to NCMEC
10	Conclusion

Our Guiding Principles



Service specific

Responses to abuse should reflect the nature of the services at issue and the ability to address the harm, while minimizing the possibility of unintended consequences.



Access to an abuse process

Complainants should have a mechanism to present their grievances to the party best positioned to address them.



Transparency

We believe in being transparent about when and how we take actions to address abuse.



Background on Content Removal and Blocking

Cloudflare offers a variety of Internet infrastructure services to users. When it comes to reports of abuse on websites that use our services, our ability to respond depends on the type of Cloudflare service at issue. Most abuse reports we receive pertain to websites that use our pass-through security and content delivery network (CDN) services, while far fewer reports relate to websites using our registrar services or our services that can be used to host content. Cloudflare's approach to reports differs depending on the nature of the services being provided.

Cloudflare offers pass-through security and CDN services to millions of websites, helping prevent cyberattacks and make the Internet more secure. In the case of websites using those services, Cloudflare is generally listed as a point of contact on relevant records. Cloudflare therefore may receive requests to remove content from our network from governments or private parties. As Cloudflare cannot remove material from the Internet that is hosted by others, we generally forward requests for removal of content to the website hosting provider, who has access to the website content and the ability to address the underlying concern.

A growing number of Cloudflare's products include storage. Examples of these [developer products](#) include Stream, Pages, Images, and R2. Consistent with the distinct legal requirements for definitively hosted content like those in the EU's DSA, Cloudflare has different terms of service and a different process for responding to legal requests or abuse complaints about content stored on our network, as opposed to content transiting or being temporarily cached on the network. If Cloudflare receives a valid takedown request regarding content that is stored on the Cloudflare network, Cloudflare will take action to limit or disable access to the content, as appropriate. This report includes details on the requests we receive to disable access to content stored on our network, described as "hosted content."

Cloudflare Registrar is an Internet Corporation for Assigned Names and Numbers (ICANN)-accredited domain name registrar that offers domain name registration and management services. Domain name registrars are generally not well positioned to address concerns about particular content on a website, as they can only take action as to entire domains. Consistent with ICANN requirements, Cloudflare takes action to mitigate technical abuse like phishing by domains using our registrar services. Cloudflare follows ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) for trademark-based domain name disputes.

The Data

Actions Taken on Hosted Content

Hosted Abuse Processes

Cloudflare maintains service-specific terms for hosted products that include content restrictions. When Cloudflare determines that content for which we provide hosting services violates the [service-specific terms](#) for Cloudflare’s developer products, we may remove, disable access, or otherwise take action to limit access to that content.

When Cloudflare receives a valid request for removal of copyrighted content hosted on one of Cloudflare’s developer products, we will provide notice to the customer and remove or disable access to that hosted content, consistent with the procedures set forth in the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512(g). If we receive a valid counter notice, we restore the removed content or cease disabling access to it, as contemplated by the DMCA.

Cloudflare follows a similar notice-and-takedown process for other types of abuse reported regarding content for which we provide hosting services. The table below includes categories that Cloudflare currently actions under our hosted abuse process. “Reports received” counts all reports received by Cloudflare, excluding reports determined to be spam. “Reports actioned” includes reports on which either Cloudflare or the customer took action. Common reasons that a report would not be actioned include that it was determined to be incomplete or otherwise invalid, or that the content at issue had already been actioned.

Year	Abuse Type	Reports Received	Total Reports Actioned	Reports Actioned at Own Initiative	Counter Notices and Appeals
H2 2024	Copyright	11,508	1,394	N/A	3
H2 2024	Trademark	3,498	1,080	N/A	1
H2 2024	CSAM	119	115	N/A	3
H2 2024	NCSEI	67	25	N/A	0
H2 2024	Threats	33	2	N/A	0
H2 2024	Phishing	170,390	51,859	385,385	456
H1 2024	Copyright	10,892	1,046	N/A	0
H1 2024	Trademark	3,888	758	N/A	0
H1 2024	CSAM	156	118	N/A	1
H1 2024	NCSEI	29	6	N/A	0
H1 2024	Threats	15	3	N/A	0
H1 2024	Phishing	143,097	34,342	0	85

Additional Context

- This year’s Transparency Report defines “reports received” to include all non-spam reports even if content had already been removed, reports were incomplete, or reports were otherwise found invalid. This results in a total number of reports received notably higher than reports actioned. For phishing reports, for example, over one-third of the reports pertained to content that had already been removed or actioned, meaning that additional action was unnecessary.
- In 2024, Cloudflare expanded the use of automated systems to respond to reports of technical abuse like phishing across our various services. In H2, Cloudflare resolved 133,102 (78%) phishing reports using automated means, up from 37% of phishing reports in H1, and the median time to action hosted phishing reports was less than one hour.
- Cloudflare relies on human review for all other forms of hosted abuse reports. In H2 2024, the median time to action hosted reports for all non-phishing abuse was 4.5 days.

Non-Hosted Restrictions of Access

Orders Relating to Pass-Through Services

Cloudflare is occasionally subject to orders from non-U.S. courts or regulatory authorities directing Cloudflare to block access to websites using Cloudflare’s CDN and security services due to copyright or other prohibited content. Because Cloudflare cannot remove content it does not host, other service providers are better positioned to address these issues. Among other things, any blocking by Cloudflare is of limited effectiveness, as a website will be accessible if it stops using Cloudflare’s network. Cloudflare therefore regularly pushes back against attempts to seek blocking orders.

When such efforts to explain why blocking is not an appropriate or effective solution are unsuccessful, we may take steps to comply with valid orders if they satisfy human rights principles relating to proportionality, due process, and transparency. In countries with laws that provide for blocking access to online content, Cloudflare may geoblock websites to limit access in the relevant jurisdiction to those websites through Cloudflare’s pass-through security and CDN services. Cloudflare has sometimes taken action to geoblock access to websites through Cloudflare’s pass-through CDN and security services, in response to orders directing Cloudflare to block through its public DNS resolver.

In countries that do not have blocking laws, Cloudflare may take steps to disable caching to websites. Disabling caching to a website does not prevent the website from being accessed through Cloudflare’s pass-through security services.

Year	Country	Type of Illegal Content	Orders	Action Taken	Number of Domains
H2 2024	Italy	Copyright	1	Geoblock	30
H2 2024	France	Illegal sports streaming	5	Geoblock	278
H1 2024	France	Illegal sports streaming	4	Geoblock	124

Mitigation of Phishing and Technical Abuse on Non-Hosted Services

As a cybersecurity company, Cloudflare has long taken steps to address technical abuse like phishing and malware across all of our services. When Cloudflare identifies technical abuse, like phishing on domains using any of Cloudflare’s services, Cloudflare places an interstitial page to warn visitors of the potentially harmful content. Because domains using Cloudflare’s registrar service generally also use our pass-through security services and CDN, Cloudflare is able to apply this approach to disrupt access to phishing and malware even for domains using Cloudflare’s registrar service. Cloudflare will suspend a domain name using our registrar services if due to the nature of the services used it is unable to place a warning interstitial page. The numbers reported below do not include actions related to content hosted by Cloudflare, which are reflected in the Hosted Abuse Process section above.

Year	Non-Hosted Actions Taken (Registrar)	Non-Hosted Actions Taken (Non-Registrar)
H2 2024	3,031	309,186
H1 2024	8,407	174,054

Requests for Content Blocking Through DNS Resolver

Cloudflare has received a small number of legal requests related to blocking or filtering content through the 1.1.1.1 Public DNS Resolver. Because such a block would apply globally to all users of the resolver, regardless of where they are located, and would affect end users outside of the blocking government’s jurisdiction, we evaluate any government requests or court orders to block content through a globally available public recursive resolver as requests or orders to block content globally.

Given the extraterritorial effect as well as the different global approaches to DNS-based blocking, Cloudflare has pursued legal remedies before complying with requests to block access to domains or content through the 1.1.1.1 Public DNS Resolver or identified alternate mechanisms to comply with relevant court orders. To date, Cloudflare has not blocked content through the 1.1.1.1 Public DNS Resolver.

Termination or Suspension of Services

U.S. Court Orders

Cloudflare is occasionally subject to third-party orders in the United States directing Cloudflare and other service providers to terminate services to websites due to copyright or other prohibited content. Termination of Cloudflare’s pass-through CDN and security services is not an effective means for addressing such content, because termination of services does not remove content from the Internet that we do not host. Other service providers are better positioned to address such websites, and it is normal for issues to be resolved even before Cloudflare takes action. Indeed, many domains that we have been ordered to terminate are no longer using Cloudflare’s services by the time Cloudflare assesses whether to take action. Nonetheless, Cloudflare may terminate services in response to valid orders that comply with relevant laws.

Year	Termination Orders	Number of Domains	Number of Accounts
H2 2024	0	0	0
H1 2024	0	0	0

Uniform Domain-Name Dispute Resolution

As an ICANN-accredited domain registrar, Cloudflare follows ICANN’s UDRP for trademark-based domain name disputes. Consistent with the policy, Cloudflare will, upon receipt of a valid UDRP verification request from an ICANN-approved dispute board: (1) Lock the disputed domain name(s) to prevent modification to the registrant and registrar information for the duration of the dispute, and (2) Unmask or provide the underlying WHOIS information to the dispute board.

Upon receipt of a valid notice of decision from an ICANN-approved dispute board, and based on the decision, Cloudflare will, as appropriate, unlock the domain to allow the respondent to manage the domain, transfer the domain to the complainant at a predetermined time to allow the respondent to initiate legal dispute with their local legal system that is within the jurisdiction of the registrar, or delete the domain.

Year	Received	Answered	In Progress	Accounts Affected	Domains Affected
H2 2024	63	63	22	70	78
H1 2024	50	50	2	57	77

Termination of Services Due to CSAM

Cloudflare terminates services, including our non-hosting services, to domains that fail to take action to remove verified child sexual abuse material (CSAM) or are dedicated to the dissemination of CSAM.

Year	Domains Terminated	Accounts Terminated
H2 2024	921	246
H1 2024	1,326	653

Voluntary Terminations

In a small number of well-publicized instances, Cloudflare has taken steps to voluntarily terminate services or block access to sites whose users were intentionally causing harm to others.

Year	Domains Terminated	Accounts Terminated
H2 2024	0	0
H1 2024	0	0

Third-Party Reporting

Reports to NCMEC

Cloudflare’s Trust & Safety team submits reports regarding CSAM to the National Center for Missing and Exploited Children (NCMEC) in response to reports submitted through our abuse form. Cloudflare offers a free CSAM Scanning Tool, which enables our customers to directly submit reports of potential CSAM material to NCMEC. After 2024 updates based on feedback from NCMEC, Cloudflare also submits third-party reports to NCMEC regarding hits by the CSAM Scanning Tool.

Year	Abuse Form Reports Submitted to NCMEC	CSAM Scanning Tool Reports Submitted to NCMEC
H2 2024	3,629	808
H1 2024	5,095	692

Conclusion

Given the vast amount of information transiting our global network, Cloudflare is mindful of the special and sensitive position we occupy with regard to our customers and the responsibilities our customers have placed on us through their trust. We will continue to publish this report on a semi-annual basis. Please be advised that we may restate data as we go forward as more complete information becomes available or if we change our classifications.





This document is for informational purposes only and is the property of Cloudflare. This document does not create any commitments or assurances from Cloudflare or its affiliates to you. You are responsible for making your own independent assessment of the information in this document. The information in this document is subject to change and does not purport to be all inclusive or to contain all the information that you may need. The responsibilities and liabilities of Cloudflare to its customers are controlled by separate agreements, and this document is not part of, nor does it modify, any agreement between Cloudflare and its customers. Cloudflare services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied.

© 2025 Cloudflare, Inc. All rights reserved. CLOUDFLARE® and the Cloudflare logo are trademarks of Cloudflare. All other company and product names and logos may be trademarks of the respective companies with which they are associated.