CLOUDFLARE

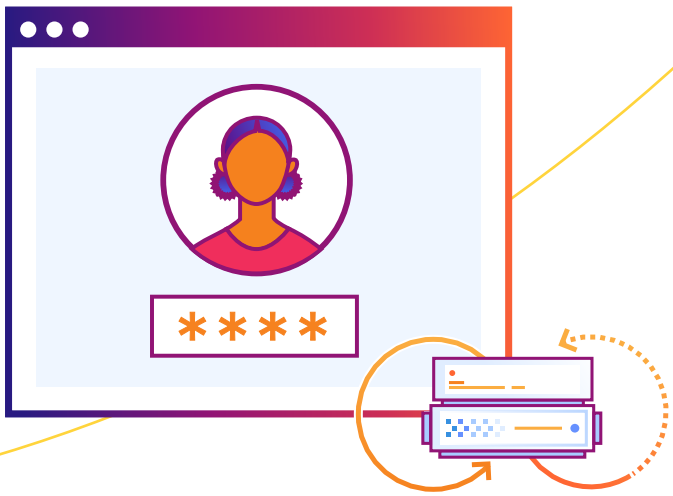
H1 2025 – Abuse processes

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, Cloudflare publishes semi-annual updates to our Transparency Report regarding our service-specific abuse processes.

We list in 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

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 hosted content like those in the EU's Digital Services Act (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 follows a notice-and-takedown process, where applicable, and 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 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 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 in response to a report. 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 at the time we reviewed the report.

Year	Abuse type	Reports received	Total reports actioned	Reports actioned at own initiative	Counter notices and appeals
H1 2025	Copyright	124,872	54,357	N/A	4
	Trademark	4,861	1,316		0
	CSAM	137	98		0
	NCSEI	49	15		0
	Threats	156	6		0
	Phishing	131,405	40,596	82,498	166
H2 2024	Copyright	11,508	1,394	N/A	3
	Trademark	3,498	1,080		1
	CSAM	119	115		3
	NCSEI	67	25		0
	Threats	33	2		0
	Phishing	170,390	51,859	194,002	456

Additional context

- In H1 2025, Cloudflare engaged with multiple rightsholders to improve the process for responding to reports of unlicensed sports streaming for copyright infringement. This engagement resulted in a significant increase in both reports of streaming and corresponding DMCA takedown actions on hosted content, which jumped from 1,394 to 54,357. We resolved 52,704 of those 54,357 copyright infringement reports using automated means, with a median time to action of less than one hour. To further mitigate abuse, we investigated indicators for the accounts and terminated R2 services of 21,218 related accounts, of which 19,817 were taken using automated means.
- In H1 2025, Cloudflare resolved 81,346 (62%) phishing reports using automated means, as compared to 78% of phishing reports in H2 2024. The median time to action hosted phishing reports was less than one hour.
- Cloudflare relies on human review for other forms of hosted abuse reports. In H1 2025, the median time to action for all hosted abuse reports that were not phishing or streaming was 5.7 days, which includes the notification period during the notice-and-takedown process.
- In H1 2025, we updated our methodology for counting actions taken against phishing on our own initiative by counting only the unique sites we took action against, as opposed to the total number of detections. This report reflects the updated numbers for both H2 2024 and H1 2025.

Government demands for takedown of hosted content

Websites using Cloudflare's services may be subject to regulatory requirements in countries around the world. Cloudflare's users are expected to comply with the relevant laws in countries which they operate.

When Cloudflare receives notice from a government that content hosted by Cloudflare violates the laws of a specific jurisdiction, we conduct an assessment of the notice. In particular, we evaluate whether the notice was issued by an official government entity, identifies a website or content hosted by Cloudflare, identifies content determined to be illegal in that jurisdiction, and directs us to remove or disable the content or website in that jurisdiction. We also assess whether it raises human rights concerns. When Cloudflare receives notice from a government that content hosted by Cloudflare violates the laws of a specific jurisdiction, we conduct an assessment of the notice. In particular, we evaluate whether the notice was issued by an official government entity, identifies a website or content hosted by Cloudflare, identifies content determined to be illegal in that jurisdiction, and directs us to remove or disable the content or website in that jurisdiction. We also assess whether it raises human rights concerns. If we determine after our assessment that action is required, we will take steps to notify our customer. If they do not address the issue within the required timeframe, we limit access to the site in the relevant jurisdiction. We may also post an interstitial page with a link to the government notice mandating the takedown. If we determine that the content also violates our Acceptable Hosting Policy, we may take action globally.

Year	Country	Orders	Action taken	Number of domains actioned by customer	Number of domains actioned by Cloudflare
H1 2025	France	1	Geoblock	1	0
	Belgium	1	Geoblock	1	0

Additional context

- In H1 2025, Cloudflare received its first government takedown notices related to sites using our hosted services for online gambling that were determined to be illegal in France and Belgium. In both cases, Cloudflare's customers responded to the notices directly by taking action to geoblock the content themselves.

Restrictions of access to non-hosted services

Orders relating to pass-through services

Cloudflare has occasionally received 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. Cloudflare resists attempts to seek these types of blocking orders because we have not found them to be an effective, long-term solution. Cloudflare cannot remove content it does not host, and other service providers are better positioned to address content removal. Blocking by Cloudflare is also of limited effectiveness, as a website will be accessible if it stops using Cloudflare's network.

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. When Cloudflare geoblocks a website, we post an interstitial page at the website with a link to the relevant order so that visitors to the site can understand why the site is not accessible.

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 content	Orders	Action taken	Number of domains
H1 2025	Italy	Copyright	3	Geoblock	33
	Belgium	Copyright	1	Geoblock	80
	United Kingdom	Copyright	1	Geoblock	13
	France	Copyright	7	Geoblock	662
H2 2024	Italy	Copyright	1	Geoblock	102

Additional context

- New legislation in South Korea requires CDNs to prohibit access through servers in South Korea to a list of websites identified by Korean authorities as illegal. The law did not take effect until H2 2025. Cloudflare plans to report on any actions it takes under this law in future Transparency Reports.
- Starting in H1 2025, Cloudflare, through its CDN and pass-through security services, geoblocked in the United Kingdom websites that are subject to copyright blocking orders issued by the High Court of Justice, Business and Property Courts of England and Wales. More details can be found here.

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 an warning interstitial page. The numbers reported below do not include actions related to content hosted by Cloudflare, which are reflected in Section 1 above.

Year	Non-hosted actions taken (registrar)	Non-hosted actions taken (non-registrar)
H1 2025	2,567	312,488
H2 2024	3,031	309,186

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 restricting access to 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 often resolve the underlying concern even before Cloudflare is expected to take action. Indeed, many domains that we have been ordered to terminate are no longer using Cloudflare's services by the time Cloudflare assesses whether action is necessary. Nonetheless, Cloudflare may terminate services in response to valid orders that comply with relevant laws.

Year	Termination orders	Number of domains	Number of accounts
H1 2025	0	0	0
H2 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
H1 2025	72	72	18	77	106
H2 2024	63	63	22	70	78

U.S. court orders to transfer domains

As a domain name registrar, Cloudflare is occasionally subject to criminal court orders relating to domain names using Cloudflare's registrar service. Cloudflare will comply with valid U.S. court orders, including seizure orders, by locking the disputed domain name(s) to prevent modification to the registrant and registrar information for the duration of the dispute and, in response to a final court decision, by transferring the domain name.

Year	Transfer orders	Number of domains transferred	Number of accounts affected
H1 2025	2	5	2
H2 2024	0	0	0

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
H1 2025	1,475	422
H2 2024	921	246

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
H1 2025	0	0
H2 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
H1 2025	4,671	731
H2 2024	3,629	808

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 semiannual basis.

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-7971.2025DEC16