



NATIONAL CENTER FOR
**MISSING &
EXPLOITED**
CHILDREN®

2023

**CyberTipline®
REPORT**



TABLE OF CONTENTS

03

Overview.....3

04

CyberTipline® Reports.....4
Electronic Service Provider Reports.....6
Referrals and Informational Reports.....8

REPORTS

10

CyberTipline® Files.....10
File Review and Triage.....11
Hash Sharing.....11

FILES

12

Removal Notices and Tracking.....12
Take It Down.....13

**REMOVING
CONTENT**

14

Domestic Response.....15
Global Response.....16
Case Management Tool.....17

**DOMESTIC
AND GLOBAL
RESPONSE**

18

OJJDP CyberTipline® Report.....18

Overview

The National Center for Missing & Exploited Children serves at the forefront of global efforts to protect children from online sexual exploitation and abuse. Our work supports law enforcement in stopping abuse and provides services to disrupt the circulation of child sexual abuse material (CSAM).

This document includes data and insights from reports of suspected child sexual exploitation made to NCMEC's CyberTipline® by the public and electronic service providers (ESPs) in 2023. Over the course of the year, NCMEC saw reports rise by over **12%** compared with the previous year, surpassing **36.2 million** reports in total. The number of files included in the reports also increased by **19%** from the previous year to more than **100 million**. The majority of reports received were related to the circulation of CSAM, but other trends indicated by the data were the continued rise in reports of financial sextortion and increasing concern related to the use of generative AI in child sexual exploitation.

From these millions of reports, NCMEC staff were able to identify and escalate for law enforcement **63,892** reports that were urgent or involved a child in imminent danger. In recent years, NCMEC analysts have observed a dramatic escalation in content demonstrating "urgent" or "imminent" threats to a child. While the overall volume of incoming CyberTipline® reports has increased by more than **20%** over the past three years, the number has grown of urgent, time-sensitive reports where a child is at risk of harm have grown by more than **140%**.

In 2023, the CyberTipline® received **36,210,368** reports of suspected child sexual exploitation.

NCMEC also continued to see inconsistencies in reporting from electronic service providers and tech companies regarding exploitation on their platforms. The majority of companies did not report at all, and many reports did not include the necessary details for NCMEC or law enforcement to take action.

In 2023, the CyberTipline® continued to see more than **90%** of reports involving the upload of CSAM by users outside the United States, fueling NCMEC's continued efforts to provide training and support to law enforcement around the world who are responding to these cases.

This report, for the first time, also lists reports on a state-by-state basis. While the majority of CyberTipline® reports involve locations outside the U.S., more than **1.1 million** reports were referred to law enforcement in the U.S. The agencies involved include the Internet Crimes Against Children Task Forces and other federal, state and local law enforcement.

Reports

CyberTipline® Reports

NCMEC's CyberTipline® is a designated reporting mechanism for the public and electronic service providers (ESPs) to report instances of suspected child sexual exploitation. It is equipped to receive reports about multiple forms of online child sexual exploitation, with CSAM making up the largest reporting category.

In 2023, the CyberTipline® received more than **35.9 million** reports that referred to incidents of suspected CSAM.

Categorization as Selected by Reporting Party

Categorization of CyberTipline® Reports	2021 Reports	2022 Reports	2023 Reports
Child Pornography (possession, manufacture, and distribution)	29,309,106	31,901,234	35,925,098
Misleading Words or Digital Images on the Internet	5,825	7,517	8,446
Online Enticement of Children for Sexual Acts	44,155	80,524	186,819
Child Sex Trafficking	16,032	18,336	17,353
Unsolicited Obscene Material Sent to a Child	5,177	35,624	45,746
Misleading Domain Name	3,304	1,948	6,883
Child Sexual Molestation	12,458	12,906	18,021
Child Sex Tourism	1,624	940	2,002
Total	29,397,681	32,059,029	36,210,368

In 2023, the CyberTipline® received over 186,000 reports regarding online enticement – a more than 300% increase from just 2021. Online enticement is a form of exploitation involving an individual who communicates online with someone believed to be a child with the intent to commit a sexual offense or abduction. Online enticement is a broad category that includes sextortion, in which a child is groomed or coerced to take sexually explicit images or even meet face-to-face with a perpetrator for sexual purposes.



[2023 Media Coverage CyberTipline® Success Stories](#)

The continued rise in financial sextortion, where an offender demands money from a child while threatening to share nude or sexual images of them with the public, has contributed to the growth of this category.

Reports of online enticement have increased more than **300% from 44,155 in 2021 to 186,819 in 2023.**

In the recent reports of financial sextortion, teen boys are most often the targets. In many cases, perpetrators will impersonate a female who wants to trade pictures. Once the targeted boy sends what the supposed female has asked for, the perpetrator will demand money or threaten to leak the images. These scenarios can happen quickly and in some cases have resulted in tragic outcomes with children taking their own lives. [Learn more about Sextortion.](#)

The CyberTipline® has also seen the alarming development of reports involving generative AI (GAI).

NCMEC is deeply concerned about this quickly growing trend, as bad actors can use GAI to create deepfake sexually explicit images or videos based on any photograph of a real child or generate CSAM depicting computer-generated children engaged in graphic sexual acts. Also highly concerning, NCMEC has received reports where families and children are being extorted by criminals using GAI CSAM for financial gain.

In 2023, the CyberTipline® received 4,700 reports of CSAM or other sexually exploitative content related to generative AI. More than 70% of GAI CSAM reports submitted to the CyberTipline® are from traditional online platforms. This statistic indicates that most GAI platforms, where the content is being created, are not reporting to the CyberTipline®.

[Read NCMEC's latest blog on this topic for more information.](#)

Electronic Service Provider Reports

The CyberTipline® receives reports from the public and electronic service providers (ESPs). To date, more than **1,600** ESPs are registered to make reports, and **16%** of these are non-U.S.-based companies that voluntarily choose to report to the CyberTipline®. In 2023, only **245** companies submitted CyberTipline® reports and five ESPs accounted for more than **91%** of the reports.

In 2023,

35,944,826 CyberTipline® reports were submitted by ESPs.

Breakdown of Public and ESP Reports

TOTAL	ESP	PUBLIC
36,210,368	35,944,826	265,542

Referrals and Informational Reports

NCMEC makes CyberTipline® reports, including our additional analysis, available to law enforcement around the world. This information helps law enforcement prioritize the most urgent cases, allowing them to take fast action when a child is most at risk. The number of cases involving a child in imminent danger have increased by more than 140% since 2021 while the total number of CyberTipline® reports has only increased by 20% in that same time.

To further assist law enforcement with prioritization, NCMEC categorizes reports it receives from the tech industry as “referrals” or “informational.” A referral is a report in which the tech company provides sufficient information for law enforcement, usually including user details, imagery and a possible location. An informational report is one in which the tech company provides insufficient information or where the imagery is considered viral and has been reported many times.

Reports without adequate information are not only ineffective in helping the child involved in the incident being reported, but they also create a larger volume of reports that must be processed to find the most critical.

In 2023, NCMEC staff escalated 63,892 reports to law enforcement in cases where the reported incident was deemed urgent or there was information that a child was in imminent danger.





NCMEC notifies companies when their reports consistently lack substantive information.

In 2023, **3.8% of CyberTipline® reports** submitted by the tech industry contained such little information that it was not possible for **NCMEC** to determine where the offense occurred or the appropriate law enforcement agency to receive the report. Among companies that made at least 100 reports in 2023, more than **80%** of the reports submitted by the companies listed below lacked adequate information to determine a location.

BigBang Media, LLC

Fediverse Communications, LLC

gayboystube

Grindr

Internet Archive

JMS Internet, Inc.

Lightspeed Systems

Megapersonals

New Meta AB

Redgifs.com

Securly

ThumbSnap

TMTG, Corp.

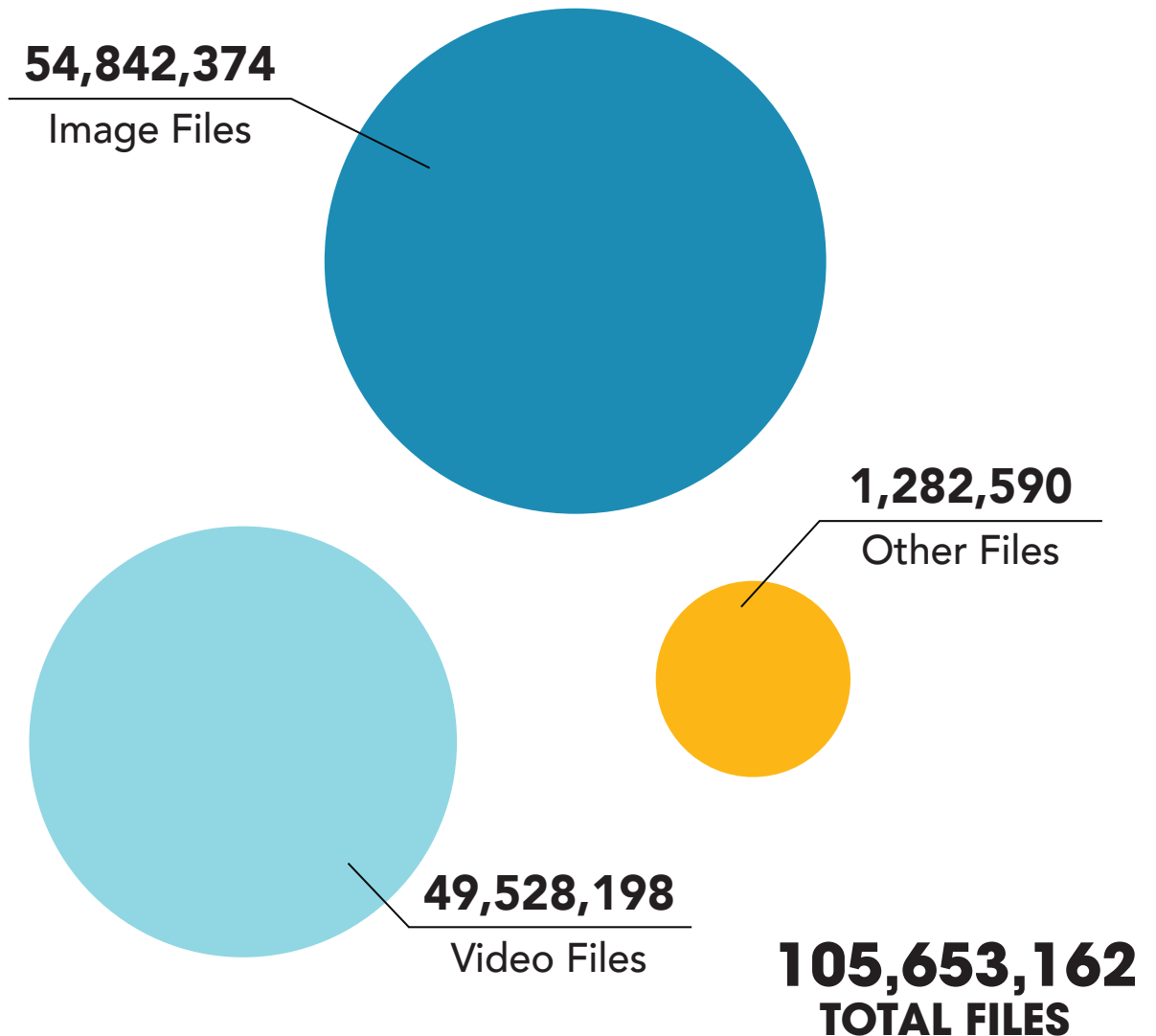
Files

CyberTipline®

Reports made to the CyberTipline® by ESPs can include images, videos and other files related to the child sexual exploitation incident being reported.

Child sexual abuse images and videos are often circulated and shared online repeatedly. CSAM of a single child victim can be circulated for years after the initial abuse occurred. One of the CyberTipline®'s critical functions is to identify unique images through the work of analysts and the use of technology. In 2023, ESPs submitted 54.8 million images to the CyberTipline® of which 22.4 million (41%) were unique. Of the 49.5 million videos reported by ESPs, 11.2 million (23%) were unique.

Data File Types Reported to the CyberTipline® in 2023



File Review & Triage

NCMEC analysts review suspected CSAM submitted by companies and label images and videos with information about the type of content, the estimated age range of the children seen and other details that help law enforcement prioritize the reports for review. For example, labels can indicate if the imagery contains elements like violence or bestiality or if it involves infants or toddlers. After labeling files, NCMEC's systems use robust hash matching technology to automatically recognize future versions of the same images and videos reported to the CyberTipline®.

The automated hash matching process reduces the amount of duplicative child sexual abuse imagery that NCMEC staff view and focuses analyst attention on newer imagery. This process helps ensure the most urgent CyberTipline® reports, where a child may be suffering ongoing abuse, get immediate attention.



NCMEC labeled more than **10.6 million files** in 2023.



Hash Sharing

Hash values are unique digital fingerprints assigned to pieces of data, such as images and videos.

They are an important tool in the effort to stop the spread of CSAM.

When an image or video is identified as containing CSAM and has been reviewed and confirmed at least three times by a NCMEC analyst, NCMEC adds its hash value to a list that is shared with technology companies.

On a voluntary basis, companies can elect to use NCMEC's hash list to detect CSAM on their systems so that abusive content can be reported and removed. As of December 31, 2023, 46 ESPs and 12 other organizations have voluntarily chosen to access this hash-sharing initiative.



In 2023, NCMEC engaged Concentrix, a customer experience solutions and technology company, to conduct an independent audit of the hashes on our list. They were tasked with verifying that all the unique hashes corresponded to images and videos that were CSAM and met the U.S. federal legal definition of child pornography. The audit, the first of its kind for any hash list, found that 99.99% of the images and videos reviewed were verified as containing CSAM.

Learn more about the audit process and their findings [HERE](#).

Removing Content

In 2023, NCMEC enhanced efforts to help stop the circulation of CSAM by working with survivors and tech companies to remove content.

Removal Notices and Tracking

When CSAM is reported by child victims, their guardians/caregivers or INHOPE member hotlines around the world, NCMEC can provide crucial support by notifying relevant platforms to review and remove any explicit images of the child.

NCMEC staff review the reported imagery and if it falls into one of the three categories below, a notification is made to the ESP where the image or video is located.

CSAM

Child sexual abuse material, which may violate federal law, a company's terms of service and/or their published community guidelines or standards.

Exploitative

Exploitative content, which depicts identified child victims, but may not reach the legal threshold of CSAM. Examples are images or videos that contain nudity, non-pornographic content associated with child sexual abuse material or otherwise sexually suggestive content of identified child victims.

Predatory Text

Text related to sexually predatory comments or personal information about an identified child victim or CSAM survivor. Personal information identifying the child in the image or video may pose safety concerns for the survivor.

2023 Total Notifications sent by NCMEC to Responsive ESPs

2023 Total Notifications sent by NCMEC to Unresponsive ESPs

In 2023, the average take-down time following a NCMEC notification for images or videos was 2.6 days.

Take It Down

Launched in December 2022, Take It Down is a free service that helps victims and survivors of online CSAM remove from the internet nude, partially nude, or sexually explicit photos and videos taken before they turned 18. Victims and survivors can remain anonymous while using this service, and they do not have to send their images or videos to anyone. Instead, Take It Down works by assigning a unique digital fingerprint – called a hash value – to the nude, partially nude or sexually explicit content. Online platforms can use Take It Down's list of hash values to detect reported images on their services allowing them to remove the content.

In 2023, Take It Down was translated into 25 languages and promoted to potential users around the world. The website recorded more than 830,000 visitors and more than 2 million page views. The majority of website visitors were based in the U.S. with India, the United Kingdom, Egypt and Canada making up the other countries with the most web visits to Take It Down. In 2023, NCMEC received over 48,000 submissions to Take It Down including over 89,000 hashes.



Domestic and Global Response

A critical function of the CyberTipline® is to refer reports to the law enforcement agency that is best able to respond to and address the issue being reported. Federal statute 18 USC 2258A requires U.S. companies to report to the CyberTipline® if they become aware of suspected CSAM on their platforms and servers. Because these companies have users worldwide and those incidents are reported to NCMEC, by extension the CyberTipline® serves as a global clearinghouse and reports are referred to law enforcement throughout the U.S. and around the world.

91.7% of CyberTipline® reports in 2023 involved the upload of child sexual abuse material by users outside of the U.S. **4.5%** of CyberTipline® reports were U.S.-based, and **3.8%** had an unknown origin.

Domestic Response

While the majority of the cases submitted to the CyberTipline® resolve outside of the United States, more than one million tips were reported among all 50 states, Washington, D.C., Puerto Rico and other U.S. territories.

Of these, **910,349** reports resolved to a specific state, but because there are many factors that go into reporting, such as IP addresses across the country, the origin of the remaining **200,000** reports cannot be confirmed. All CyberTipline® reports are made available to law enforcement in the U.S. including Internet Crimes Against Children Task Forces and other local, state and federal agencies.

When the state is unknown, the reports are made available to federal law enforcement in the U.S. NCMEC works closely with law enforcement throughout the U.S. providing training and resources to support their response to CyberTipline® reports.



2023 CyberTipline® Reports by State

Global Response

With more than 91% of reports being referred outside the U.S., NCMEC has forged partnerships with law enforcement in 160 countries and territories that receive CyberTipline® reports, including Interpol and Europol.

Interpol also assists in the dissemination of CyberTipline® report information to certain countries where NCMEC doesn't have a direct connection to law enforcement. These important connections to law enforcement allow for a quick and seamless referral of CyberTipline® reports to help ensure children around the world are safeguarded – and offenders are held accountable.

NCMEC staff also provide CyberTipline® trainings in other countries, mentor non-governmental organizations (NGOs) seeking to expand technical and operational capacities within their own hotlines, educate on best practices and share child safety and prevention material around the world.

We collaborate with dozens of global NGOs, including WeProtect, ECPAT, International Justice Mission (IJM), Internet Watch Foundation, the Canadian Centre for Child Protection, UNICEF and many others. NCMEC is also a founding member of INHOPE, a global network of 50 member hotlines across six continents.



2023 CyberTipline® Reports by Country

Case Management Tool

The NCMEC Case Management Tool (CMT), developed with support from the U.S. Office of Juvenile Justice and Delinquency Prevention (OJJDP) and Meta, enables NCMEC to share reports securely and quickly with law enforcement around the world.

The CMT allows law enforcement in the U.S. and abroad to receive, triage, prioritize, organize and manage CyberTipline® reports. Through robust and customizable display data, dashboards and metrics, law enforcement users can tailor their report queue for more immediate triage and better response.

It also helps police agencies refer reports to other law enforcement agencies for a more targeted response. The system helps NCMEC notify law enforcement of high priority reports.

In support of easier adoption and use by international users, the CMT fields and interface are available in eight languages (English, Spanish, French, German, Portuguese, Arabic, Hindi and Thai) with additional translations planned. Domestically, all Internet Crimes Against Children Task Forces, the FBI and Homeland Security Investigations also have access.



OJJDP CyberTipline® Report

In consultation with the Office of Juvenile Justice and Delinquency Prevention (OJJDP), NCMEC prepared an additional transparency report regarding CyberTipline® activity in 2023. It is a complementary resource to the report on this page and contains additional detail about the reports made to the CyberTipline® in 2023.



2023 NCMEC/OJJDP Transparency Report



NATIONAL CENTER FOR
**MISSING &
EXPLOITED**
CHILDREN®

2023

**CyberTipline®
REPORT**

[NCMEC.org/CyberTiplineData](https://www.ncmec.org/CyberTiplineData)

Copyright © 2024 National Center for Missing & Exploited Children.
All rights reserved.

This project was supported by Grant No. 15PJDP-23-GK-04261-MECP awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this program are those of the author(s) and do not necessarily reflect those of the Department of Justice.