United States Senate Committee on the Judiciary

"Protecting Our Children Online Against the Evolving Offender"

December 9, 2025

Testimony of Lauren Coffren, Executive Director, Exploited Children Division
National Center for Missing & Exploited Children

I. Background

The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization created in response to an unthinkable tragedy. In 1981, 6-year-old Adam Walsh was with his mother in a Florida shopping mall when he vanished without a trace. Adam's parents, Revé and John Walsh, endured 10 excruciating days searching for Adam before he was found murdered 100 miles away. The Walshes channeled their grief and came together with other child advocates to create NCMEC in 1984. Over the past 41 years, NCMEC has grown into the nation's largest and most influential child protection organization. Today NCMEC fulfills its Congressionally-designated mission to help find missing children, combat child sexual exploitation, and prevent child victimization through five core programs of work relating to: (1) missing children; (2) exploited children; (3) community outreach; (4) educational and professional resources; and (5) family support.

As technology has become more sophisticated, online threats against children have become more complicated and pernicious. As part of NCMEC's Congressionally-mandated role to combat child sexual exploitation, we have identified, tracked, and worked to combat evolving forms of online child sexual exploitation for over 25 years. Over the past year, NCMEC has witnessed dramatic increases in new forms of exploitation, including online enticement and financial sextortion; sadistic online exploitation perpetrated by violent online groups; and the emergence of generative artificial intelligence (GAI) technologies capable of creating child sexual abuse material (CSAM) and facilitating child sexual exploitation. In 2024, NCMEC saw dramatic increases in reports relating to these new forms of abuse – a 192% increase in reports concerning online enticement; a 200% increase in reports relating to sadistic online exploitation; and a 1,325% increase in reports with a GAI nexus, compared to 2023. Already this year yet another disturbing new trend is emerging in the form of AI chatbots and AI companion technology that can sexually exploit children.

The increasing volume of reports relating to these emerging forms of egregious online abuse is horrifying, but, unfortunately, anticipated. Children have been sexually exploited online for decades, and offenders are known to be among the earliest adopters of new technology. Yet Congress has not passed comprehensive federal measures to protect children from online sexual exploitation. Today, new technology and online platforms are not required to incorporate safety-by-design measures; online platforms are not required to be transparent regarding child safety issues, substantively report

incidents to NCMEC's CyberTipline, or take efforts to detect the sexual exploitation of children on their services; and victims have no ability to hold online platforms that facilitate their exploitation legally accountable. Most members of the public are outraged by the volume of children subjected to extreme sexual exploitation online. However, the trend of tech-savvy offenders using new methods to sexually exploit children online will continue unabated until we have laws and regulations in place to curtail these evolving offenders and ensure safer environments online for children.

II. CyberTipline

For over 27 years, NCMEC has operated the CyberTipline, the centralized online mechanism for members of the public and online platforms to report incidents of suspected child sexual exploitation, including: the online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. Online platforms are statutorily required[1] to submit a report to NCMEC's CyberTipline when they have actual knowledge of an apparent violation of federal law relating to child pornography, child sex trafficking, or online enticement of children on their platforms. This reporting requirement drives submission of reports to the CyberTipline but does not require online platforms to take proactive steps to detect child sexual exploitation, remove content after it has been reported, or submit timely, substantive, consistent information to the CyberTipline.

Since the CyberTipline was created, NCMEC has responded to 220 million reports relating to child sexual exploitation, which provides us with a unique vantage point to identify emerging exploitation trends so we can alert law enforcement and the public. While the number of CyberTipline reports submitted to NCMEC in 2024 decreased from 2023,[2] NCMEC continued to see an influx of reports relating to children at risk for imminent harm, which requires urgent review and response. On average, NCMEC's systems alerted our staff to over 1,400 reports a day that contained chat messages or images indicating the child was at imminent risk and the report was time-sensitive. Many reports escalated for imminent harm to a child involve newly emerging crimes relating to online enticement/financial sextortion, sadistic online exploitation, and generative artificial intelligence sexual exploitation.

Children in every community and state across the country are regularly victimized by online exploitation, including newer crimes relating to financial sextortion and sadistic online exploitation. Attached as Exhibit A are summaries of reports received by NCMEC relating to children in each state represented by members of this Committee.

I. Emerging Trends

Most online offenders exploit children online for their own sexual gratification. In recent years, however, NCMEC has seen the emergence of new types of exploitative crimes against children driven

[1] 18 U.S.C. § 2258A.

[2] In 2024, NCMEC's CyberTipline received 20.5 million reports, a significant decrease from the 36.2 million reports received in 2023. Even accounting for the decrease attributable to a new, beneficial "bundling" feature to streamline reporting of "viral" reports, NCMEC's 2024 CyberTipline numbers reflect a decrease of 7 million reports. NCMEC attributes this overall decrease to reduced reporting from a handful of online platforms and implementation of end-to-end encryption across multiple online platforms, which blinds companies to child sexual exploitation on their services.

by financial motives and nihilistic goals to control, degrade, and torture children. For these offenders, the sexual exploitation of a child is no longer the end goal, but a heinous stepping-stone along a larger online campaign to achieve financial gain through blackmail or inflict systematic abuse against vulnerable children. The impact of these crimes is so significant that, for the first time this year, NCMEC released mid-year CyberTipline report statistics to alert the public to the dramatic increases in crimes involving online enticement/financial sextortion, sadistic online exploitation, and the use of GAI to facilitate child sexual exploitation.

Congress and this Committee have taken decisive action in recent years to address specific issues threatening child safety online through passage of the REPORT Act and the TAKE IT DOWN Act. Each of these bills, as further discussed below, addressed discrete online child sexual exploitation crimes. The STOP CSAM Act,[3] a comprehensive child protection bill, is still pending after passing unanimously out of this Committee for the past two terms. This bill would materially change the course of how we as a nation combat online child sexual exploitation, by addressing a range of improvements and modifications to allow for earlier intervention against child exploitation, including rapidly evolving crimes; better protections for child witnesses and children receiving restitution; improved transparency and reporting by online platforms; and the ability of victims to hold accountable those who facilitate their online exploitation. NCMEC supports the STOP CSAM Act as consequential legislation that needs to be passed as soon as possible.

A. Online Enticement of Children

Online enticement involves an offender communicating online with a child to commit a sexual offense. Sextortion is a form of online enticement where a child is threatened or blackmailed, most often with potential distribution of nude or sexual images in which they are depicted, by an offender who demands additional sexual content or sexual activity from the child.

Offenders often target a child to entice online by deceiving or coercing them to share a nude or explicit image after making the child believe they are communicating with someone they know or trust as a romantic interest. In many cases, offenders use images of another person and communicate through fake accounts. This type of victimization takes place across online platforms, including social media, messaging apps, and gaming platforms.

The volume of online enticement reports received by NCMEC is alarming and continues to increase. In 2024, NCMEC received more than 546,000 reports relating to online enticement. This is a 192% increase in reports compared to 2023. In the first six months of 2025, NCMEC received 518,720 reports relating to online enticement – a 77% increase compared to the 292,951 online enticement reports received in the first six months of 2024.

[3] The STOP CSAM Act was introduced by Senator Hawley and Ranking Member Durbin; is supported by many members of the Senate Judiciary Committee; and passed unanimously out of this Committee in June 2025. The STOP CSAM Act strengthens CyberTipline reporting; creates civil liability for online platforms and app stores that intentionally, knowingly, or recklessly promote or aid and abet violations of child sex trafficking, online enticement of a child, or child pornography; establishes transparency requirements for online platforms relating to child safety issues; and provides updates and new protections for child witnesses and children receiving restitution as a result of their victimization.

The increase in online enticement reports submitted to NCMEC over the past year is largely due to the success of the REPORT Act enacted in May 2024. While some online platforms voluntarily reported online enticement incidents to NCMEC, this bill for the first time made it mandatory for online platforms to report online enticement to NCMEC's CyberTipline.[4] As a result of this increased reporting, more children in online enticement situations are receiving intervention and services and law enforcement is alerted to more offenders attempting to victimize children online.

I. Financial Sextortion

Financial sextortion is a form of sextortion in which the offender demands money or something of financial value (i.e., gift cards) in exchange for not distributing nude or sexual images in which the child is depicted. Typically, online payments are demanded through peer-to-peer electronic payment systems, such as Cash App, PayPal, or Apple Pay. Similar to online enticement, offenders often target a child who initially believes they are communicating with someone connected through mutual friends or who is a new romantic interest. Unlike offenders who are sexually motivated to prey on children, financial sextortion offenders are driven by financial gain and often participate in decentralized, loosely-coordinated domestic or international criminal networks.[5]

The crime of financial sextortion uniquely targets teenage boys between the ages of 14 and 17 – often with tragic outcomes – and often is perpetrated very quickly, sometimes within hours. Since 2021, NCMEC is aware of more than three dozen teenage boys who have taken their lives as a result of being victimized by financial sextortion, however there likely are more cases that have not been identified as relating to financial sextortion. These boys are often athletes and other high-performing teenagers with large social circles. They are targeted by offenders with incessant, aggressive threats of public exposure, shame, arrest, and loss of their future goals if they do not comply with escalating demands for money.[6] The coerced suicide in most of these cases differs from other suicides among young people in that most children victimized by financial sextortion did not have known mental health conditions or previous suicidal ideation.

In 2024, NCMEC received more than 33,000 reports relating to financial sextortion. This is a 24% increase in reports compared to 2023. In the first six months of 2025, NCMEC received 23,593 reports

---

[4] The REPORT Act, introduced by Senator Blackburn and Senator Ossoff and supported by many members of this Committee, also made it mandatory for online platforms to report child sex trafficking incidents to NCMEC. As a result of this new requirement, child sex trafficking reports to NCMEC increased by 952% from the first half of 2024 to the first half of 2025 (5,976 reports in the first half of 2024; 62,891 reports in the second half of 2025). NCMEC provided reporting guidance for online platforms regarding online enticement and child sex trafficking to help ensure actionable reporting of these incidents to the CyberTipline (Guidelines on Identifiers of Online Enticement and Child Sex Trafficking).

[5] Press Release, U.S. Dep't of Just., Nigerian Brothers Sentenced in Sextortion Scheme that Resulted in Death of Teen (Sept. 5, 2024), https://www.justice.gov/archives/opa/pr/nigerian-brothers-sentenced-sextortion-scheme-resulted-death-teen.; Press Release, U.S. Dep't of Just., Ivory Coast Man Charged with Participating in a Sextortion Scheme that Caused the Death of a North Dakota Teenager (Jan. 22, 2025), https://www.justice.gov/usao-nd/pr/ivory-coast-man-charged-participating-sextortion-scheme-caused-death-north-dakota; Press Release, U.S. Dep't of Just., Nigerian Man Sentenced to Six Years in Prison for Cyberstalking and Other Charges Related to the Sexual Extortion and Death of a Local Young Man (Oct. 28, 2025), . https://www.justice.gov/usao-edpa/pr/nigerian-man-sentenced-six-years-prison-cyberstalking-and-other-charges-related-sexual.

[6] Wetzel, Dan, *The predatory web of sextortion increasingly ensnares young athletes,* ESPN, Aug. 10, 2025, https://www.espn.com/high-school/story/_/id/45852691/fbi-extortion-online-youth; Halliday, Josh, *FBI and NSPCC alarmed at 'shocking' rise in online sextortion of children*, The Guardian, Aug. 9, 2025; Hale, Rachel, *These young men were tricked into sending nude photos, then blackmailed: the nightmare of sextortion,* USA Today, April 22, 2025.

of financial sextortion – this represents a 70% increase in reports compared to the 13,842 reports received in the first six months of 2024.

The aggressive tactics used by financial sextortion offenders often include sending dozens of messages in less than an hour, starting a countdown for the child to comply, or sending details about the child's friends or family to demonstrate who they will contact if the child does not comply. The examples provided below are from chat messages reported in CyberTipline reports relating to financial sextortion submitted to NCMEC:

Financial Sextortion Report Example #1

SUSPECT: Confirm it
CHILD VICTIM: It will charge my dad
SUSPECT: Confirm it wtf
CHILD VICTIM: I'm actiallly going to kill myself
SUSPECT: Okay let me send them out then idc
SUSPECT: You send it and we're done and I'll delete your stuff
CHILD VICTIM: I can't
SUSPECT: Ok bet
CHILD VICTIM: I'm actually gonna kill myself my life is over thanks for ruining it
SUSPECT: Ok

Financial Sextortion Report Example #2

SUSPECT: If u try to f*** with me or u try to block me I will make sure I ruin ya life and I post it on bbc new just cooperate with me imma leave u to go ok once u block me I will ruin ya life and u will go to jail and your parents will not like that so just cooperate with me so I will jot ruin ya life
SUSPECT: Just cooperate with me I will just keep your s*** here only if u cooperate with me
SUSPECT: Once u f*** with me I will post it now bbc news
CHILD VICTIM: You have nudes a 16 year old minor, so actually, you would go to jail.
SUSPECT: Are u ready to cooperate
CHILD VICTIM: I can't believe this 18 year old asked me for nudes
CHILD VICTIM: I'm not even old enough to give consent
SUSPECT: I'm a guy
CHILD VICTIM: EVEN WORSE
SUSPECT: And I will make sure I ruin ya life
SUSPECT: Just cooperate with me or your parents see your s*** online
CHILD VICTIM: I don't care
SUSPECT: U want to blame your self right
SUSPECT: Just pay me and we are done
CHILD VICTIM: No one will miss me when I'm gone tomorrow
CHILD VICTIM: I hope you like having photos of a dead boy
CHILD VICTIM: 8:19 AM tomorrow. Make sure to remember me. You might be the only one that will

Today, the harms created by financial sextortion are exacerbated by offenders' use of GAI technology to create fake nude or sexually explicit images to sextort and threaten child victims. Now an offender

does not need to engage with a child online and deceive them into sending an explicit image; instead the offender can locate an innocuous image of the child on social media, create an explicit digital forgery depicting that child, and sextort the child based on the GAI digital forgery.[7] In the first six months of 2025, NCMEC received 75 CyberTipline reports from members of the public that involved GAI being used as part of financial sextortion. The dangers represented by financial sextortion are so severe that in recent years several U.S. and international federal agencies have issued notices warning of the dangers presented to children from this crime and calling on law enforcement and financial institutions to detect and disrupt the crime when it occurs.[8]

II. Sadistic Online Exploitation

For years NCMEC has responded to child sexual exploitation, however the emergence of sadistic online exploitation (SOE), a recent trend perpetrated by violent online groups,[9] has led to the most egregious exploitation reports NCMEC has ever seen. SOE offenders often exhibit nihilistic or anarchic ideological beliefs and work together in small groups, even from different countries, to target and perpetrate extreme and degrading abuse on children, including coercing children to:

- Create and share sexually explicit content
- Self-mutilate, including carving the names of the offenders onto their bodies
- Harm, mutilate, or kill animals
- Physically and sexually abuse, harm, and mutilate other children (including younger siblings)
- Self-immolate and/or commit suicide through other means
- Threaten members of their community (i.e., threaten school shootings)

Children who are especially vulnerable – whether due to social isolation, depression or mental health issues, or eating or self-harm disorders – are often uniquely targeted by SOE offenders. Based on NCMEC's review of CyberTipline reports relating to SOE incidents, girls are most often victimized (84% of victims) from ages 14-17 (75%); 11-13 (21%); and some victims under 10 years old (4%). Offenders are predominantly male (88%), with a majority over 18 years old (75%), but many under 17 years old (25%).

These groups target children on popular online platforms, including most prominently Discord, X, Roblox, and gaming sites. While online enticement offenders often target children for sexual gratification or in the case of financial sextortion, financial gain, SOE offenders are motivated to force

---

[7] Valdes, Nicole & Breen, Kerry, *A teen dies after being blackmailed with A.I.-generated nudes. His family is fighting for change*, CBS News, May 31, 2025.

[8] "FinCEN Issues Notice of Financially Motivated Sextortion", September 8, 2025, FinCEN Issues Notice on Financially Motivated Sextortion | FinCEN.gov; "International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis", February 7, 2023, International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis — FBI; "HSI, federal partners issue national public safety alert on sextortion schemes", December 19, 2022, Archived: HSI, federal partners issue national public safety alert on sextortion schemes | ICE.

[9] One of the most prominent SOE groups, 764 group, was created by Bradley Cadenhead, a 15-year-old living in Stephenville, Texas. The group's name was derived from the first three digits of Cadenhead's Stephenville ZIP codes (76401 and 76402) for. In 2023, Cadenhead was prosecuted and sentenced to 80 years in prison. While 764 was one of the first SOE groups, other violent extremist groups continue to vie to become the "worst of the worst." Davis, Patricia, *Using sextortion to groom kids for violence, pain*, NCMEC Blog, August 28, 2025, https://www.missingkids.org/blog/2025/using-sextortion-to-groom-kids-for-violence-pain.

terror and extreme physical abuse on children.[10] Offenders frequently swarm a child victim online, making rapid-fire threats to kill a child's family, swat[11] their family house, or disclose the child's personal information unless the child acquiesces to comply with their demands.

The examples provided below are from chat messages reported in CyberTipline reports relating to SOE incidents submitted to NCMEC:

SOE Report Example #1

SUSPECT 1: i found her address
SUSPECT 1: @everyone someone add her back
SUSPECT 1: [child's full street address]
SUSPECT 2: Took her that long to figure that out
SUSPECT 2: Damn it
SUSPECT 2: F*** she blocked me
SUSPECT 2: WE ARE READY TO SWAT
SUSPECT 3: I know your address
SUSPECT 3: Leave and ill f****** kill you.
SUSPECT 2: LAST CHANCE
SUSPECT 2: DO WHAT WE SAID AND THEY WONT SIMPLE
SUSPECT 3: They will f****** die.
CHILD VICTIM: I don't want my family to die
SUSPECT 3: Write all of our names in s*** then
CHILD VICTIM: I did nothing wrong
CHILD VICTIM: No
* * *
SUSPECT 3: HOLD UP A F****** PAPER THAT SAYS [suspect screenname] GROOMED ME
CHILD VICTIM: What did I do
SUSPECT 2: NOW
SUSPECT 3: isnt that hard.
SUSPECT 3: time is ticking.
CHILD VICTIM: I did nothing wrong
SUSPECT 2: DO IT
SUSPECT 2: LAST CHANCE
CHILD VICTIM: I am innocent
SUSPECT 3: DO WHAT WE F****** SAID.
CHILD VICTIM: No
SUSPECT 3: YOUR GETTING F****** SWATTED
SUSPECT 2: DO WHAT WE SAID

[10] Levine, Mike, *'Modern day terrorism': How the online extremist network 764 is threatening teen lives,* ABC News, November 18, 2025, https://abcnews.go.com/US/modern-day-terrorism-online-extremist-network-764-threatening/story?id=127528502.

[11] Swatting is a malicious act that can involve placing false calls to emergency responders to report a false ongoing crisis at a specific location. The goal of swatting is to provoke a significant law enforcement response, creating chaos and potentially resulting in violence. https://www.dhs.gov/sites/default/files/2025-04/25_0325_fps_swatting.pdf.

SUSPECT 3: THATS IT.
SUSPECT 1: YOUR PARENTS ARE GONNA BE DEAD AND LIFELESS

SOE Report Example #2
SUSPECT 1: I went to vc that cutslut … Carved my whole name onto her … She cut for me
SUSPECT 2: we need videos of content … and i think if we host more cutshows it will grow us more
SUSPECT 1: We need members
SUSPECT 2: we need to know if she does good bloodsigns and good cuts
SUSPECT 1: ill promo on tele[gram]
SUSPECT 3: do u guys send animal cruelty to people?
SUSPECT 2: No … I love cats thats why i dont get animal content … [suspect screenname] doesnt extort for his animal content … he just kills them
SUSPECT 3: how is 764 a satanic cult of people didn't sell their souls?
SUSPECT 4: I cant bring myself to kill an animal
SUSPECT 2: You can worship stuff without selling their souls … Most groups labeled as satanic really aren't … Most of these kids just wanna be edgy and get bloodsigns and shit … but you can use these egirls blood for better astrial projection and power
SUSPECT 5: Got a new content slut in training

SOE Report Example #3 (from a CyberTipline report submitted by a child victim)
"[he] posed himself as a weight loss coach...made me send nude photos that had my face in them...He sent me my address saying he would hurt me and send the photos to all my friends and family...the only way that he wouldn't do that was if i video called him and hung myself from my wardrobe completely naked, in order to kill myself.

SOE reports to NCMEC continue to increase dramatically. In the first six months of 2024, NCMEC received 508 reports of SOE, and in the first six months of 2025, the CyberTipline received 1,093 reports – a 115% increase. Overall NCMEC has seen a 1,500% increase in SOE reports between 2022 and 2024.

In September 2023 and again in March 2025, the FBI's Internet Crime Complaint Center issued Public Service Announcements to raise awareness about the emerging threats of SOE. Additionally, FBI Director Kash Patel specifically raised the rising crisis presented by SOE in his opening remarks at this Committee's September 16, 2025, FBI Oversight hearing.[12] Given the extraordinary and diverse harm caused by SOE offenders – ranging from threats and coercion leading to sexual exploitation, brutal self-harm, and the abuse of animals – a careful analysis must be undertaken to ensure that our current laws provide prosecutors and law enforcement with sufficient legal tools to quickly respond and thwart this multifaceted online abuse of children.

Significantly, until this year, most SOE-related reports were submitted by the child victim or a parent or caregiver after they learned of their child's self-harm or suicide attempt. In 2024, members of the

[12] "We're going after the new form of what I refer to as modern day terrorism in America. 764, crimes that involve harming our children by going after them online, causing self-mutilation, suicide, sexual abuse and steering them in the wrong direction. Currently, we have 3500 international terrorism investigations. Specifically, we have in this country, 1700 domestic terrorism investigations, a large chunk of which are Nihilistic Violent Extremism (NVE) those who engage in violent acts motivated by deep hatred of society, whatever that justification they seem is, the FBI has seen a 300% increase in cases opened this year alone versus the same time last year." *Senate Judiciary Committee Oversight Hearing of the Federal Bureau of Investigation.*, 119 Cong. (2025) (statement of Kash Patel, Dir. of the FBI).

public submitted 69% of SOE reports, while online platforms submitted only 31%. It is unacceptable that online platforms have failed to take essential steps to detect, disrupt, and report SOE activity on their services and instead we rely on child victims and their friends and parents/caregivers to report these incidents. There is a significant gap in the industry's awareness and response to evolving exploitation on their platforms. Given NCMEC's role as the national clearinghouse on child exploitation issues, in August 2025, NCMEC convened representatives of international, federal, and state law enforcement and representatives from online platforms to focus on emerging trends relating to SOE and to facilitate solution-oriented strategy sessions on how best to combat this new evolution of child sexual exploitation offenders.

B. Generative Artificial Intelligence Child Sexual Abuse Material

Sexually explicit and nude images of children created with generative artificial intelligence (GAI) constitute child sexual abuse material and/or obscene visual representations of the sexual abuse of children under the law. It is essential that our federal and state laws recognize the harm and proliferation of GAI sexually abusive imagery and the importance of preventing emerging GAI technology from being used to exploit children and that communities, schools, and parents understand how to recognize and educate children on the exploitative harms that can arise from GAI.

Offenders actively use GAI to exploit children in a variety of ways, including the following:

- **Text to Chat:** Entering text to get a chat model to pretend it is a child and engage in sexually explicit chat.

- **Text to Text:** Entering text to generate guides/tutorials/suggestions on how to groom, sexually abuse, torture, and kill children.

- **Text to Image:** Entering text prompts to generate CSAM or alter previously uploaded files to make them sexually explicit.

- **Image to Image (altering known CSAM to create new CSAM**): Uploading known CSAM to generate new CSAM based on existing images, including altering or adding new abusive elements (e.g., bondage or other forms of abuse) to existing images.

- **Image to Image (altering innocuous image to create exploitative image):** Uploading innocuous images of a child to generate sexually explicit or exploitative images for personal gratification and/or to humiliate and embarrass the child. Sometimes GAI is used in this manner to perpetrate financial sextortion against a child (e.g., nudify/unclothe/undress apps).

CyberTipline reports related to GAI are skyrocketing, and NCMEC estimates that we have not yet begun to see the true impact of this technology on the sexual exploitation of children online. In 2024, NCMEC received more than 67,000 reports related to GAI, and in the first six months of 2025, NCMEC received 440,419 reports – a 6,343% increase. This increase is partially attributable to a

small handful of AI companies that have implemented screening methods to detect and report known CSAM to NCMEC.[13]

These GAI-related reports also include the distressing trend of school-related incidents in over a dozen states in which an offender – often another student – uses a "nudify" GAI tool to create nude images from innocuous images of a child and circulates them among other classmates. The TAKE IT DOWN Act enacted in May 2025, will play a significant role in ensuring that more incidents involving nude and sexually exploitative images involving a child (whether GAI or real imagery) can be federally prosecuted and victims have a process to seek removal of these images from the Internet.[14] The bill provides crucial tools for law enforcement and prosecutors to intervene at the earliest indication that a child is being exploited, especially through enticement/sextortion, and to safeguard the child and investigate the offender. NCMEC is aware that many cases involving nude or sexually exploitative material escalate to more egregious abuse and early intervention can protect children from further harm. The TAKE IT DOWN Act also requires online platforms to create a process to enable victims and authorized individuals to report real or GAI sexually abusive images and request removal of the imagery. This is the first notice and removal process under federal law relating to child sexual exploitation images and provides much-needed hope for victims seeking to remove their online explicit images.

The TAKE IT DOWN Act marked a crucial step towards closing the gap that existed in protecting children from GAI sexual exploitation. However, additional legislation in the form of the ENFORCE Act[15] is needed to ensure that obscene visual depictions of child sexual abuse, which include many GAI sexually abusive images that do not meet the strict legal definition of child pornography, are accorded the same legal protections and tools as CSAM.

It is critical for lawmakers and the public to recognize that GAI CSAM is CSAM and impacts children and communities just as authentic CSAM does. GAI CSAM also complicates victim identification efforts, taking time and resources from NCMEC and law enforcement trying to determine if a child is real and in need of rescue. It is imperative that policymakers ensure that the law keeps up with the challenges GAI poses to the safety of children.

II. NCMEC's Programs to Combat Evolving Child Sexual Exploitation Trends

As the national clearinghouse on missing and exploited children issues, NCMEC is uniquely situated to identify trends and create unique programs and educational resources to address the evolving threats to children online. These programs include direct services to child victims, therapeutic support for families and survivors, and prevention and educational materials.

[13] The volume at which known CSAM is detected by a small number of AI companies underscores the prevalence of offenders utilizing AI technology to exploit children and the tremendous gap in both content moderation techniques and safety by design adoption by AI companies.

[14] The TAKE IT DOWN Act was introduced by Senator Cruz and Senator Klobuchar and supported by many members of this Committee.

[15] The ENFORCE Act was introduced by Senator Cornyn, Senator Blumenthal, Senator Lee, and Senator Kennedy.

A. NCMEC's Take It Down Service

NCMEC created the Take It Down service in 2022, to help minors remove and stop the online sharing of nude, partially nude, or sexually explicit images or videos in which they are depicted. The service is anonymous and relies on image hash-matching, so a child does not have to share their images or videos to participate, and no one at NCMEC receives or views the child's images.[16] Today over a dozen online platforms have chosen to participate in the Take It Down program by using hash values submitted by minors to NCMEC's service to detect and remove reported images or videos.

B. Professional Training

Professionals who work on child exploitation issues, whether law enforcement, prosecutors, or child welfare professionals, have a tremendous amount of critical work and limited resources. In order to address emerging trends in child exploitation, those working in this space must have specific knowledge of these crimes, understand how they present, and who is likely to be targeted.

In order to meet the needs of those in our communities who keep children safe every day, NCMEC hosts both in-person training sessions at our Alexandria, VA, headquarters and throughout the United States at our regional offices and partner agencies as well as offers online courses through NCMEC Connect. This program is designed to provide easy access to training and resources for professionals on the frontlines enabling them to learn at their convenience.

C. NCMEC's Online Safety Education Programs

NCMEC provides a wide variety of online safety education programs with age-appropriate videos and activities to help children understand potential online risks and empower them to prevent victimization by making safer choices on and offline. Life in 2025 is driven by technology and providing appropriate information about threats online and how to handle them to children at a young age is critical to keep children safe in our digital world.

NCMEC utilizes the trends it sees in CyberTipline reports to consistently create new materials based on emerging threats. This year, NCMEC released new episodes of *Into the Cloud*, our flagship online safety product for children ages 11 and under, addressing online enticement, sextortion, and GAI victimization. Each episode is between 3-6 minutes and can be used at home or in the classroom to help educate children through corresponding discussion guides and associated games and activities.

III. Conclusion

Online exploitation of children is escalating in volume and becoming more virulent and extreme. This trend will not abate until Congress requires online platforms to adopt safeguards, incentivizes safety by design, and provides law enforcement, prosecutors, survivors, and supporting non-profits with the needed tools to protect children from online sexual exploitation and combat the evolving techniques offenders are utilizing to harm children. Given NCMEC's unique role operating the CyberTipline, we

[16] NCMEC's Take It Down service enables a child with a nude or sexually explicit image of themselves on their device to upload a hash value (a digital fingerprint uniquely identifying an image) of the image and transmit it to NCMEC. NCMEC compiles hash values submitted to Take It Down and makes that list available to participating online platforms to scan their public, unencrypted services to detect, report, and remove instances of the image if it appears on their services.

are uniquely positioned to identify patterns and emerging exploitation trends. We look forward to working with this Committee to continue to share trends and data derived from our work to combat online child sexual exploitation and to craft legislative solutions that can ensure children are safe online and in the real world.

Exhibit A

NCMEC State-Specific CyberTipline Report Examples
Relating to Financial Sextortion and/or Sadistic Online Exploitation of Children

Alabama

In April 2024, NCMEC's CyberTipline received a report from Discord concerning a suspect in Alabama who asked a female child to harm themselves multiple times, including cutting themselves on a video call without wearing a shirt. The suspect and child discussed possessing and sharing CSAM and bestiality content with each other, including in exchange for cash or Robux (virtual currency used on the Roblox website), and meeting for a sexual encounter and to molest infants. The suspect frequently discussed alleged prior experience and an interest in killing and molesting infants, children, and animals. The suspect also expressed desire to "shoot up" an elementary school (stating, "when i finish ima rape one of them"). This report was made available to law enforcement in Alabama based on the apparent location of the suspect and Argentina based on apparent location of the child victim based on the apparent location.

California

In September 2025, NCMEC's CyberTipline received a report from Snapchat detailing sextortion relating to a suspect and child victim located in California. The report contained a chat log detailing the suspect's request for $700 from the child or the suspect would share explicit content in which the child was depicted online. The chat log displays frequently seen tactics in sextortion cases, including a countdown in the chat to create a feeling of urgency for the child. The chat log also reflects the suspect asking for money in gift cards because the minor may not have access to a bank to send money. The suspect also details the proof they need that the minor is going to the store to purchase the gift cards, including asking for images or videos of them obtaining the gift cards. This report was made available to law enforcement in California based on the location of both the suspect and child victim.

Connecticut

In September 2025, NCMEC's CyberTipline received a report from Instagram concerning a suspect associated with a recognized alias used in sadistic online exploitation (SOE) of a child. The suspect asked the child for explicit sexual imagery and self-harm (including on their genitals). The report indicates the child may have sent explicit images and a bloodsign (a symbol, name or other marking created using the child's blood or blood from an animal or another person the child has been coerced to harm). Despite being blackmailed, including through a threat to be swatted, the child victim appears to request that the suspect extort another child victim with them. This is an example of how SOE child victims can become perpetrators themselves as they become more familiar with the "Extortion Com", an element of the 764 network. Another child victim in Connecticut was blackmailed, including through distributing personal information, swatting, and doxxing). Despite the abuses, the child victim exhibited loyalty to the suspect,

stating "i would actually kms for u [...] like actually cut open my stomach and bleed out on cam for u and spell ur name out w my internal organs". This report was made available to law enforcement in Connecticut, Florida, Indiana, Ohio, and the United Kingdom based on apparent locations of the reported suspect and child victims.

Delaware

In June 2025, NCMEC's CyberTipline received a report from Instagram concerning sextortion that resulted in the child victim making statements of suicidal ideation. The reported chat log includes the suspect threatening to share explicit imagery of the child for financial gain, while the child victim expresses statements of suicide after the blackmail begins. This report was made available to law enforcement in Delaware based on the apparent location of the child victim and law enforcement in Nigeria based on the apparent location of the suspect. The following is an excerpt of the reported chat log:

SUSPECT: "Imma send it to all groups your family all school member am gonna post it"

CHILD VICTIM: "Bro your gonna make me kill myself bc of that"

CHILD VICTIM: "I'm being so fr"

SUSPECT: "About to post 😂"

CHILD VICTIM: "Stop stop stop"

SUSPECT: "Pay me"

Florida

In August 2025, NCMEC's CyberTipline received a report from a member of the public relating to an offender located in Florida who was associated with the sadistic online exploitation (SOE) group 764, and potentially was the leader of an extortion ring known as 1378. The reporting individual stated that the offender "preys on children online specifically with mental illnesses and causes them to cut themselves, kill their pets, go on cam and show their genitalia". The reporting individual also shared that child victims who did not comply with the offender's demands were threatened to be "swatted" or to have their personal information leaked. This report was made available to law enforcement in Florida based on the apparent location of the incident.

Hawaii

In August 2025, NCMEC's CyberTipline received a report from Instagram concerning financial sextortion of a minor by an offender who appeared to be located in Cote D'Ivoire, which along with Nigeria is a leading country for offenders engaging in financial sextortion. The offender asked the child victim if they "would like a video of this kind coming from you to be published and your dignity be flouted?" and told the child "[I]f you try to escape, to play hard, to stand or disconnect you will really see what I am capable. So do not try to run away.", and "Try not to finish the call on Faceboo k , otherwise you are a dead man,

or even to retire as friends on Facebook or even to block me, if you think to do it, you only make worse the situation?". This report was made available to law enforcement in Hawaii based on the apparent location of the child victim and law enforcement in Cote D'Ivoire based on the apparent location of the suspect.

Illinois

In April 2025, NCMEC's CyberTipline received a report from Instagram concerning a suspect that blackmailed a child victim with an alleged unclothed image depicting the child and doxxing information. The child victim has appeared in several reports, as recently as September 2025. In these reports, the child victim has been reported as a suspect, child victim, and chat participant among other possible sadistic online exploitation (SOE) associates, with imagery including a lorebook (a collection of sexually explicit/self-harm imagery of the victim and messages between the victim and the offender). The child was blackmailed, including doxxing and swatting, asked to perpetrate a bomb threat, expressed suicidal ideation, and asked to self-harm. These reports were made available to law enforcement in Illinois and Texas when the child victim made a suicide threat.

Iowa

In September 2025, NCMEC's CyberTipline received a report from a victim's parent after their child was contacted via direct message on Instagram by someone requesting a nude image. The child victim shared an image and was blackmailed "5 minutes later." The offender offered to send explicit content if the victim first sent their own image, threatened to share the victim's image if requests to send money to the offender were not complied with, and threatened to bring shame to the victim by sharing the victim's images. This report was made available to law enforcement in Iowa based on the apparent location of the child victim.

Louisiana

In September 2025, NCMEC's CyberTipline received a report from Instagram detailing financial sextortion of a child victim located in Louisiana by a user based in Nigeria. The report contained uploaded files of explicit content and what appeared to be images of the victim's friend list. Sextortion offenders often show their victims a list of the "friends" or users that may receive the child's explicit content if the child does not send money to the offender. The suspect requests $200, and then another $100, while the child victim expresses suicidal ideation. Chat logs contained in the report show the offender expressing a sense of urgency, a common tactic to make the child panic and send the requested money. This report was made available to law enforcement in Louisiana and to law enforcement in Nigeria based on the apparent location of the suspect. The following is an excerpt from the chat log included with the report:

SUSPECT: I got all your friends here
SUSPECT: Am sending your sh*t to 50 of your female friends rn
CHILD VICTIM: Please stop, I'm sorry
SUSPECT: Get me 200 fast

SUSPECT: And I delete your shit
SUSPECT: What do you use for payment
CHILD VICTIM: I have no money!!
SUSPECT: Pick up fast
SUSPECT: Fast
CHILD VICTIM: I'm gonna kill myself
CHILD VICITM: I'm gonna kill myself
SUSPECT: You think am joking 👺 👺
SUSPECT: Watch out
CHILD VICTIM: Im about to shoot mussels in the head
SUSPECT: Am sending it to my website rn 202396928

Minnesota

In March 2025, NCMEC's CyberTipline received a report from Facebook detailing sextortion of an apparent minor by an offending account in Nigeria, which along with Cote D'Ivoire, are the countries in which the vast majority of financial sextortion offenders reported to NCMEC's CyberTipline are located. The chat log provided in the report shows the offender encouraging the exchange of exploitative or explicit content and then immediately threatening to post the imagery unless the minor meets the suspect's monetary demands, usually via electronic payments or the purchase of gift cards. This report was made available to law enforcement in Minnesota based on the apparent location of the child victim and to law enforcement in Nigeria based on apparent location of the suspect.

Missouri

In May 2025, NCMEC's CyberTipline received a report from Discord after they were contacted by law enforcement in Missouri concerning a suspect that used similar strategies online as groups involved in sadistic online exploitation (SOE) use to exploit child victims. The child victim discussed issues they were having with their parents, and the suspect validated the child's experience and reciprocated by sharing their own vulnerabilities. The suspect also sought to communicate with the child victim's friends to gain their trust. When faced with disapproval from the friends, the suspect and child victim discussed plans to conceal their relationship. Ultimately, the relationship was used to coerce the child victim to self-harm their genitals. This report was made available to law enforcement in Ohio based on the apparent location of the child victim, and later to law enforcement in Missouri. The following is an excerpt from the chat log included with the report:

CHILD VICTIM: brother you encouraged me to carve "daddys slut" into my fupa.... thats not rlly a good example of treating smn right
CHILD VICTIM: also youre literally 20. im 17, still a minor
CHILD VICTIM: youre very lucky im not one of those pedo hunters bc i could report u to the cops rn but i wont
CHILD VICTIM: bc i believe in recovery and second chances

CHILD VICTIM: youre not a bad guy
CHILD VICTIM: i know youre better than this
SUSPECT: Constructive cutting, rather than random. And in my defense, you could have said no, but you enjoyed it
CHILD VICTIM: not rlly
CHILD VICTIM: i only did it to make you happy, which i obv failed to do

New Jersey

In July 2024, NCMEC's CyberTipline received a report from a child victim in New Jersey who stated, "my life is on the line." The child victim detailed persistent exploitation by the suspect which included: extortion over the course of a year, harassment with CSAM of others, enticement to self-harm and commit suicide, leaking of their own explicit imagery, harassment and swatting of their family, calls to child protective services and hotlines, bomb threats to their school, and accessing their online accounts. The child victim reported the suspect's chat logs from three different electronic service providers. Two months later, NCMEC's CyberTipline received a report from a friend of the child victim concerning the same situation. The report was made available to law enforcement in New Jersey based on the location of the child victim and to law enforcement in North Carolina based on the apparent location of the suspect.

North Carolina

In September 2025, NCMEC's CyberTipline received a report from Instagram concerning a suspect located in North Carolina who was engaging in sadistic online exploitation (SOE), including soliciting CSAM and self-harm content from multiple child victims, including one child who discussed suicidal ideation and past attempts to overdose. The chat logs reflect one child victim stating: "i wnana make myself throw up for u and do inappropriate thinfs with [myself] and send u stuf and do whatevr u want i will be a really good girl for u and iHope u newever leave me or i guess i will jsut be realy sad because i never sender nudes a lot and now i send [nudes] and ill be so attached to u". Another child victim stated: "yeah one of my ex bf said he extorted liek a year before beimg my bf n was "retired" next thing ik im being extorted". The suspect and another SOE associate discuss their plans to further exploit both child victims. This report was made available to law enforcement in North Carolina, California, Michigan, and the United Kingdom based on apparent locations of the reported users as well as the FBI.

Rhode Island

In April 2025, NCMEC's CyberTipline received a report from Discord detailing solicitation of self-harm content and enticement for a child to engage in eating disorder behavior. The chat excerpt below shows the offender enticing the child to "starve" themselves:

SUSPECT: "also u gotta like 100% starve more often its cute af"
CHILD VICTIM: "yes tmrw and the rest of this week I'm going to my parents forced me to eat already"
SUSPECT: "thats soo boring of them"
CHILD VICTIM: "ik they so fake that's why they all big"

SUSPECT: “oh dangg they fake”
CHILD VICTIM: “fake for not letting me starve”
SUSPECT: “oh yhh they boring asf LMAOO”
SUSPECT: “good parents would let u do what u want like starve smoke cut do drugs n shi”

The report contains additional chat logs in which the suspect encourages the child victim to purge and track calories and requests for images showing bones beneath body parts, such as a ribcage. This report was made available to law enforcement in Rhode Island based on the apparent location of child victim and to law enforcement in Ireland based on the apparent location of the suspect.

South Carolina

In October 2024, NCMEC’s CyberTipline received a report from Instagram concerning a suspect in South Carolina, who blackmailed, requested sexually explicit content and bloodsigns, and cutsigns evidencing self-mutiliation, and suggested suicide to child victims. Some child victims may have sent such content and/or expressed suicidal ideation. One child victim offered their passwords and shared their address with the suspect, and another stated, “Imliteryly relapsing over ts pls u mean the world to me I just didn't want u to move on please we can talk about this we can fix this Caleb I promise just talk to me”. The suspect is also alleged to have “swatted” and leaked personal content relating to other child victims. The suspect’s alias appears several times in other CyberTipline reports relating to sadistic online exploitation (SOE) CyberTipline reports and self-harm files. This report was made available to law enforcement agencies in several states, including South Carolina, where an arrest was made, Georgia, Kentucky, Ohio, Virginia, and the FBI.

Tennessee

In November 2024, NCMEC’s CyberTipline received a report from Discord regarding a suspect who engaged in sexual conversations with, solicited CSAM from, and repeatedly pressured child victims to self-harm. One child victim said they would create a smaller cut on their skin because they “ALMSOT FAINTED TODAY". To “get back into 764” the suspect instructed the second child victim to self-mutiliate and to “start stabbing ur wrists [...] n then let the blood leak everything [....][expletive]go get a bible and bleed over it”. The suspect and child victims frequently discussed and shared images/videos of several other child victims that were blackmailed and enticed to self-harm and take their own lives. This report was made available to law enforcement in Tennessee, New York, and Pennsylvania based on the apparent locations of reported users. The following are excerpts from the chat log included in this report:

SUSPECT: CUT 764 ON UR STOMACH
SUSPECT: then do like
SUSPECT: repent x skin
SUSPECT: on the side
CHILD VICTIM: nah bro what
CHILD VICTIM: –[Expletive] ALL MY OTHER CUTS HAVENT HEALED

[...]
SUSPECT: your 9yr old brother
SUSPECT: ur 10 yr oldbrother
SUSPECT: both in one sign
CHILD VICTIM: no
SUSPECT: cut my name into blood
SUSPECT: then use the blood
SUSPECT: to
SUSPECT: write
SUSPECT: repent is pure evil
[...]
SUSPECT: im going to find you
SUSPECT: kidnap you
SUSPECT: and rape you everyday
SUSPECT: for like a few months
CHILD VICTIM: ok
SUSPECT: until i get scared of the cops
SUSPECT: and kill you
SUSPECT: wait
SUSPECT: kill you or you just tell the cops you ran away

Texas

In June 2025, NCMEC's CyberTipline received a report from Discord concerning several individuals involved in sadistic online exploitation (SOE) against child victims. One child victim in Texas was potentially already self-harming before being asked to engage in further self-harm behaviors by the suspect. The victim was told to cut "down the road [...] not across" and to overdose with "as many as u can [...] beacuse u talked to another man". The suspect also sought to isolate the child victim by having them remove online connections and accessing their account(s). The suspect eventually asked the child victim to self-mutiliate with "as much blood as possible" and record themselves swallowing numerous pills. This report was made available to law enforcement agencies in multiple states and countries, including Texas, Alabama, California, Illinois, Missouri, Canada, and the United Kingdom based on the apparent location of the users.

Utah

In June 2025, NCMEC's CyberTipline received a report from a child victim relating to a sextortion scam in which the child was enticed to send a nude image to another user. The victim stated that the offender threatened to "send it out over Instagram to my friends and family". The child victim also described being contacted by the offender on "multiple emails" while also receiving calls and texts with continued threats. This report was made available to law enforcement in Utah, who provided feedback indicating an arrest was made, and also to law enforcement in the Philippines based on the apparent location of the suspect.

Vermont

In October 2025, NCMEC's CyberTipline received a report from the FBI detailing financial sextortion of a minor. The reporting individual appears to be the child victim who disclosed: "I sent nudes to a telegram account that I found on tiktok that was posing as a 17-year-old girl. They threatened to share it to everyone who I follow on tiktok if I did not pay them. I sent them a steam gift card but then they just demanded more money." This report was made available to law enforcement in Vermont based on the apparent location of the child victim.