REFINITIV EXPERT TALK

Combatting child sexual abuse in a digital era

Author

Gökçe Arslan Kumar
Threat Finance Research Manager, APAC, Refinitiv

Online child sexual exploitation includes crimes related to possessing, distributing, producing, and accessing child sexual exploitation material, online grooming and luring[1] and it is growing at an alarming pace. In its latest 2020 report, the not-for-profit Internet Watch Foundation found a 16% annual increase in child sexual abuse imagery online.[2]

Introduction

The exponential increase in internet access globally, including for children, has caused increased exposure of children to criminal grooming and exploitation. The COVID-19 pandemic has exacerbated the situation by restricting the movement of many children who are now consuming even more content online. COVID-19 further imposed extraordinary economic stress on many families (especially in countries at greatest risk of child sexual exploitation), making them more vulnerable to exploitation. Moreover, rapid technological advancements have made this criminal content not only easier and cheaper to produce and consume but has helped to mask illicit activity, due to the heightened use of encryption and other technologies designed to avoid detection.

[1] https://www.fintrac-canafe.gc.ca/intel/operation/exploitation-eng
[2] https://www.iwf.org.uk/sites/default/files/inline-files/PDF%20of%20IWF%20Annual%20Report%202020%20FINAL%20reduced%20file%20size.pdf

International Centre™ FOR MISSING & EXPLOITED CHILDREN

REFINITIV®

A comprehensive approach to tackling these crimes with a focus on public-private partnerships is needed.

The regulatory response

The aim of protecting children resonates deeply with global regulators, as well as reporting entities, all of whom are aware of the deep social impact that such heinous crimes can cause.

A focus on the financial aspect of online child abuse would require reporting institutions to be aware of payments linked to the access, consumption, production, or distribution of abusive material.

Regulators have been quite active in analysing all suspicious transactions reports and identifying financial indicators which may suggest transactions are linked to child exploitation. Some of these indicators released by AUSTRAC, FINTRAC and AMLC include:[3]

- Low value transactions
- Transfers to a recognised higher-risk jurisdiction for child exploitation
- No work or family links between the sender and the destination country
- Attempts to obfuscate the sender's identity, such as name variations
- Transactions involving individuals who are mentioned in adverse media/official sources as accused or convicted of child sexual exploitation related offenses.

As suggested by the sample of indicators mentioned, the identification and reporting of suspected transactions linked to child abuse is a challenging task for reporting institutions.

These challenges include:

- The lower value of transactions associated with child abuse makes it harder for transactions to be detected and reported as suspicious.
- Higher risk jurisdictions sometimes include countries where limited information is available in the public domain. This challenge increases in countries where most credible sources are in the local language. As a result, it is difficult to comply with the critical requirement to identify links to child exploitation in information available in the public domain, where such links are included in relatively obscure local language sources.
- Naming conventions need to be understood to avoid screening errors and obtain accurate results based on each institution's name matching thresholds. As every "suspicious transaction" starts with a "positive" hit on screening systems, an inability to understand naming conventions may result in missed alerts.
- A close look at the financial indicators and regulatory guidance around false positive handling demonstrates that a holistic picture of every case needs to be established before a reporting institution files a suspicious transaction report. But if every institution sets automated screening systems to very fuzzy settings to eliminate risk and the risk intelligence data, they screen against is neither populated with rich identifiers nor provides the granularity needed to pinpoint relevant content sets, compliance teams could quickly become overwhelmed with hundreds or even thousands of false positives a day. This is a serious outcome as it may lead to human errors (such as closing some alerts without the thorough investigation being demanded by regulators) or the use of automated solutions which aren't fit for purpose. Considering the reputational damage associated with even the inadvertent facilitation of child abuse, some reporting institutions might opt for "de-risking" where customers, which fit some criteria for being "high risk" in relation to child abuse, might be denied financial services based on suspicion alone. This is another unintended consequence of sifting through a high number of false positives.
- While reporting entities are at the frontline of combating child abuse, none of them have all

[3] https://www.austrac.gov.au/sites/default/files/2021-09/Other%20Domestic%20Banks_Risk%20Assessment_2021.pdf/
https://www.fintrac-canafe.gc.ca/intel/operation/exploitation-eng/
http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20OSEC%20AN%20EMERGING%20RISK%20AMID%20THE%20COVID19%20PANDEMIC.pdf

the information they need to prevent these crimes. They are expected to regularly monitor increasingly dynamic and complex typologies related to child abuse and to submit fast and high-quality suspicious transaction reports to regulators. This requires not only close collaboration between them and other public and private organisations studying such typologies, but also information sharing with other financial institutions, which itself creates regulatory hurdles in most countries.

Welcome to Video

In 2015, a South Korean national created a website, Welcome to Video (WTV), on the encrypted portion of the internet, Dark Net, where sexually explicit videos of children and teens could be bought using Bitcoin. In March 2018, after expanding its user base to 38 countries, it was finally shut down in a complex operation involving law enforcement agencies from several countries. A few points which made this case unique include:

1. The site had 1.3 million Bitcoin addresses registered and received more than 353,000 USD worth of Bitcoin between 2015-2018.[4]
2. The site was the largest in terms of the sheer volume of child abuse material stored which exceeded 8 terabytes. According to the US Department of Justice, this website was "among the first of its kind to monetise child exploitation videos using Bitcoin".[5]
3. A total of 338 users of this website spread across 12 countries were arrested and charged for child exploitation related offenses. This required extensive collaboration between law enforcement agencies and many other nonprofit and private organisations in many countries who came together to stop these crimes.
4. While most users were charged with child abuse related offenses, some were also charged with other offenses, including money laundering.
5. The National Center for Missing and Exploited Children (NCMEC) analysed over 250,000 videos associated with this site and found that over 45% contained new images that were previously not known to exist.[6] This is pertinent at a time when data privacy legislation impacts any potential action which could be taken by technology providers regarding child abuse material online. This also reinforces the need for stronger child protection laws to, for example, mandate the use of scanning devices for material relating to child abuse by technology companies.[7]

The successful shut down of this website was an unmitigated success for law enforcement and other agencies who were also able to rescue 23 minor victims in multiple countries who were being abused by users of this website.

However, the case does raise some challenges in terms of how reporting institutions could detect such transactions going forward. These include:

1. The identification of individuals convicted of such crimes. Though the arrests took place in 12 countries, many of those convicted criminals would receive different sentences depending on their specific country's legislation. The operator of the website was sentenced to 18 months imprisonment in South Korea and his extradition to the US was also denied. It is reasonable to assume that a US conviction for the same crime would have led to a harsher sentence. This raises a challenge for reporting institutions to ensure that they have access to relevant data to mitigate the risks of doing business with such offenders.
2. Identifying individuals connected to such crimes. As the arrests occurred in multiple countries with identifiers of offenders (such as local aliases, and DOBs) most likely appearing in local sources, a comprehensive effort is required to not only find as much identifying information as possible, but also to link these individuals to the same case so a holistic picture of the potential network can be established. This is especially true for certain countries such as South Korea where local naming conventions lead to a handful of family

[4] https://blog.chainalysis.com/reports/chainalysis-doj-welcome-to-video-shutdown
[5] https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child
[6] ibid
[7] https://www.europarl.europa.eu/news/en/headlines/society/20210701STO07548/parliament-approves-rules-to-tackle-child-sexual-abuse-online

names accounting for the majority of names in the country. A lack of secondary identifiers would therefore cause an exponential rise in false positives, which could overwhelm compliance teams. Data curated from credible local sources would undoubtedly be helpful for reporting institutions to flag any transaction linked to individuals/entities involved in this network.

Reporting institutions must screen against high quality AML risk intelligence data, curated from credible sources (both local and global). Several critical criteria would need to be met for this data to be fit for purpose including:

1. Availability of data on individuals/entities identified in local adverse media/official sources as being reportedly linked to child abuse, to enable the institution to appropriately assess the associated risk.
2. All naming variations of individuals and entities involved in child abuse need to be available for screening. This should include native alias screening or screening against names in local languages which must be carefully curated by specialist research teams with these language skills as they are a strong identifier in and of itself.
3. Data needs to be rich in secondary identifiers such as date of birth/identification number so that false positives are kept to an absolute minimum.
4. Data needs to help connect the dots by identifying relationship networks between criminals, including highlighting front companies and associates.
5. Data needs to be very structured and granular and should allow for increased configurability to enable reporting institutions to identify specific content (such as that linked to child abuse) and select and filter data based on their own risk-based approach and legal/regulatory requirements.

With an extensive research infrastructure involving hundreds of trained analysts located in multiple global offices, fluent in more than 65 global languages and aware of specific risks in every country and region, the World-Check Risk Intelligence database plays a critical role in providing regulated institutions with data to tackle the challenges mentioned above. This helps reporting institutions to meet their customer and third-party due diligence screening obligations and prevent child abuse and fight financial crime.

Another critical component of this fight is partnerships between like-minded organisations in the public and private sectors.

One such partnership initiated by AUSTRAC in 2017 is the Fintel Alliance, which includes major banks, remittance service providers and gambling operators in Australia along with law enforcement and security agencies in Australia and overseas.[8] Since Fintel Alliance's establishment, there has been a 945% increase in major banks filling suspicious transaction reports in relation to suspected child abuse which has led to arrest of offenders in Australia and the rescue of many children overseas.[9] This partnership indicates the real value of data sharing initiatives in combatting child abuse, but more can certainly be done to remove obstacles to this type of collaboration.

OUR RESPONSE: WORLD-CHECK RISK INTELLIGENCE DATA AND SICs

What are the Special Interest Categories (SICs)?

The Special Interest Categories (SICs) are the classification of information obtained from media sources, sanctions or law & regulatory enforcement sources to indicate the nature of alleged or actual offences and/or information relating to the status of explicit & implicit sanctions that may pertain to data subjects in World-Check Risk Intelligence data records.

What are the benefits of Special Interest Categories in World-Check One?

A structured taxonomy of SICs will assist customers in the segmentation of data based on their own requirements. SICs provide more detailed category information concerning the nature of the potential risk associated with World-Check Risk Intelligence data records. As an example, an individual involved in "possession and distribution of sexually explicit videos of children online" would be flagged with different SICs such as "Exploitation of Children", "Sexual Exploitation", "Illegal Possession" and "Human Rights Violations", each of which tagging highlight different aspects of this crime. Users can filter for specific information using Case Match view filters or relevant Report extracts. Additional Admin options will also provide greater flexibility in setting screening parameters which may aid in reducing the volume of matches.

[8] https://www.austrac.gov.au/about-us/fintel-alliance

Conclusion

There is no disputing either the alarming prevalence of child sexual exploitation material online or the significant harm that it inflicts on society. The ongoing pandemic, the use of anonymisation technologies, the pervasive influence of social media applications amongst children and their abusers, the disjointed legislation in different countries including those with non-dissuasive penalties for child abuse, and the general public's preference for personal privacy in their use of technology are all factors that have contributed to this crisis.

While there is broad consensus on the urgency of tackling child abuse online amongst regulators, reporting institutions and even technology providers, a concerted effort by them is needed to make a meaningful impact.

Regulators are right to demand that reporting institutions understand all red flags associated with child abuse and analyse every transaction closely to identify and manage risks appropriately. But they must also ensure that data sharing partnerships that would further enhance partnerships and knowledge sharing between financial institutions are made possible by encouraging necessary legislative changes.

Reporting institutions must ensure that they not only collect excellent KYC data but that they screen it against comprehensive risk intelligence data which would enable them to meet their legal and regulatory obligations.

About Refinitiv, an LSEG business

Refinitiv, an LSEG (London Stock Exchange Group) business, is one of the world's largest providers of

financial markets data and infrastructure. With $6.25 billion in revenue, over 40,000 customers and 400,000 end users across 190 countries, Refinitiv is powering participants across the global financial marketplace. We provide information, insights and technology that enable customers to execute critical investing, trading and risk decisions with confidence. By combining a unique open platform with best-in-class data and expertise, we connect people to choice and opportunity – driving performance, innovation and growth for our customers and partners.

About International Centre for Missing and Exploited Children (ICMEC)

The International Centre for Missing & Exploited Children (ICMEC) is a non-governmental organization, headquartered in the United States, with offices representing Asia Pacific, Latin America & the Caribbean, and Australia. ICMEC works to make the world a safer place for children by defending against child sexual exploitation, abuse, and the risk of going missing. ICMEC works with partners around the world to develop research, technologies, and educational resources to aid in the search and recovery of children who are missing, fight child sexual exploitation, and empower caring professionals, institutions, and communities to safeguard children from all forms of sexual abuse.

Based on ICMEC's success in building stakeholders' interest around collaboration on data-driven initiatives, ICMEC Australia is now looking to deliver data collaboration initiatives and best practices that enhance the detection and investigation of crimes against children online within the bounds of the law; and initiate & facilitate collaborative action to reduce the volume of child exploitation crimes within and from Australia.