University of Nottingham
Rights Lab

GLOBAL
FUND
TO
END
MODERN
SLAVERY

Investigation into financial transactions used in the online sexual exploitation of children

The state of evidence

September 2023

Content notice

This report deals with the topic of online sexual exploitation of children (OSEC) and includes reference to abuses experienced by children in this context. The report does not recount the specific experiences involved in OSEC cases. However, it does describe types and patterns of behaviour associated with OSEC in general terms.

Authorship and acknowledgements

This report was funded by the Global Fund to End Modern Slavery (GFEMS). The opinions, findings, and conclusions stated herein are those of the author(s) and do not necessarily reflect the views of GFEMS.

This report was reviewed by lived experience experts, whose inputs and perspectives are integrated throughout the document. Special thanks to Ruby, Liberty, and Joy for their invaluable insights. Special thanks to Ruby, Liberty, and Joy for reviewing and advising on this report.

Rights Lab project team:

Dr Ergul Celiksoy, Rights Lab Research Fellow in Modern Slavery and Criminal Justice, University of Nottingham (lead author)

Dr Katarina Schwarz, Rights Lab Associate Director (Law and Policy) and Associate Professor of Antislavery Law and Policy, School of Law, University of Nottingham

Contents

Figures

Tables

Text boxes

Table of abbreviations

ACCCE	Australian Center to Counter Child Exploitation
AFP	Australian Federal Police
AMLC	Republic of the Philippines Anti-Money Laundering Council
AUD	Australian Dollars
AUSTRAC	Australian Transaction Reports and Analysis Centre
CPS	Crown Prosecution Service (UK)
CSAM	Child Sexual Abuse Material
CSEM	Child Sexual Exploitation Material
CVC	Convertible virtual currency
EFC	European Financial Coalition
EMI	Electronic Money Issuer
ESP	Electronic Service Provider
ESW	Egmont Secure Web
FBI	Federal Bureau of Investigation (US)
FinCEN	Financial Crimes Enforcement Network (US)
Fintech	Financial technology
FIU	Financial Intelligence Unit
ICT	Information Communication Technology
IRS-CI	Internal Revenue Service Criminal Investigation (US)
IWF	Internet Watch Foundation
MSB	Money Service Business
NBI-AHTRAD	National Bureau of Investigation Anti Human Trafficking Division (Philippines)
NCA	National Crime Agency (UK)
NCMEC	National Center for Missing and Exploited Children (US)
NGO	Non-Governmental Organization
NPCC	National Police Chiefs' Council (UK)
OSEC	Online Sexual Exploitation of Children
PHP	Philippine Pesos
PII	Personally Identifying Information
PNP-WCPC	Philippine National Police - Women and Children Protection Center
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
URL	Uniform Resource Locator
USD	United States Dollars
VPN	Virtual Private Network

1. Introduction

To reach the UN Sustainable Development Goal Target 16.2 of eliminating all forms of exploitation, abuse, trafficking, and violence against children, the international community must join forces to tackle the growing global problem of online sexual exploitation of children (OSEC), including the use of live streaming. (IJM, 2020, p. 13). However, in the past decade, law enforcement agencies have noticed an upsurge of exploitative activities with a commercial scope. Generally, the offender pays through a money transfer agency to the trafficker who has access to exploited children in order to generate child sexual exploitation material (CSEM). This material is then transmitted from live streaming video communications platforms. These activities are classified as trafficking in persons according to the Palermo Protocol (IJM, 2020, p. 16).

Live streamed OSEC is different from other online child sexual abuse crimes in two ways. First, it is financially motivated; and second, it involves both physical and virtual components (Cubitt, Napier, & Brown, 2021). The facilitators of OSEC are often family members of the child victim and commit physical sexual offences for financial reward (Huikuri, 2022, p. 11). The victims and abusers are usually located in developing countries, such as the Philippines, yet the issue is also seen in other countries and regions (Europol, 2020, p. 39). OSEC ‘customers’ (demand-side offenders) order illegal virtual sessions, which include requests for sexual violence to be conducted on child victims, without them being physically present (Huikuri, 2022, p. 11).

The ability to live stream and create content on demand has enabled remote customers of OSEC to take an active role in directing the actions of traffickers and children. However, most Electronic Service Providers (ESPs) with the ability to provide live streaming services do not supervise these data flows to detect CSEM. This is because live streams typically do not generate stored images or videos, which are the typical indicators of these offenses. Established detection methods for CSEM are therefore unable to detect them (IJM, 2020, p. 16). Identifying occurrences of OSEC is further complicated for ESPs, law enforcement, and other interested parties because evidence of the crime is often found across multiple platforms, including social media applications, messaging transfer agents, and computers/mobile devices (ibid).

Given that OSEC is a financially motivated crime, the increased utilization of digital and mobile payments has been of great benefit to OSEC offenders, enabling them to both make and receive payments quickly and without identification (ECPAT, INTERPOL and UNICEF, 2022, p. 75). Research has found that a range of payment methods are utilized to facilitate OSEC, including money transfer services, digital currencies, and Bitcoin (Desara, 2019, p. 32). The financial sector has a major part to play in the fight against OSEC because financial intelligence can be a powerful tool for law enforcement personnel to identify perpetrators of such abuse (ECPAT France, 2022, p. 82).

2. The distinct nature of OSEC crimes

As noted above, OSEC is a distinct crime compared to other forms of child sexual exploitation offences both online and offline. In this section, we highlight the main features of OSEC relevant to understanding the crime and designing effective responses.

The modus operandi of OSEC is both straightforward and merciless. Perpetrators from all over the globe look for traffickers on the web in countries like the Philippines, paying them to stream live the abuse and exploitation of minors in the manner directed by the far-off offender in real time (IJM, 2020, p. 12). Demand-side offenders make use of popular internet sites with live video and chat capabilities to issue explicit and detailed abuse commands, and the sexual abuse is broadcasted for the offender's sexual gratification on a "pay-per-view" basis (ibid)[1].

2.1. The supply side of OSEC

OSEC is a broad term used to describe a range of activities that involve the online sexual abuse of minors. These activities include, but are not limited to, possession and distribution of CSEM, live streaming of child sexual exploitation, solicitation of minors to produce new CSEM, and grooming of minors for contact abuse. OSEC is especially concerning due to its young victims, the high frequency of family involvement, and the acceptance of this activity in some communities (Dedase-Escoton, et al., 2020, p. 18).

A number of studies examined the supply side of OSEC and found that this crime is carried out in three district ways: (i) individual operations; (ii) family-run operations; and (iii) cybersex dens (Ramiro, et al., 2019; Varrella, 2017; Terre des Hommes, 2013).

2.1.1. Individual operations

In individual operations, child victims are the ones who initiate contact with the demand-side perpetrator without the assistance of a third-party facilitator (Dedase-Escoton, et al., 2020, p. 18). Individual operations refer to children taking part in an activity independently, with no direct involvement from another individual. These children are often from homes that are not well-functioning and may endure physical or emotional mistreatment. They may find out about the activity by themselves through searching online or be encouraged to participate by their peers. This activity can occur in public places such as internet cafés, or in more private settings, such as those where a 'Piso Net' is available. This is a type of computer where one peso can be inserted into a machine to access the internet for a limited time. In some cases, the internet cafe may be open all night and not have an owner monitoring the area (ECPAT France, 2022, p. 21).

[1] 'Pay-per-view' is a type of distribution model where viewers can purchase and watch specific content, typically live events or special programming, by paying a one-time fee per view. In OSEC cases, offenders usually pay for each OSEC session where the sexual abuse is imposed on children.

2.1.2. Family-run operations

Research has revealed that the majority of OSEC cases are usually family-oriented crimes, with the victim's own biological parents or relatives being the perpetrators of the abuse (IJM, 2020, p. 51; Garcia & Manikan, 2014, p. 30; Terre des Hommes, 2013). In this form of abuse, mothers or other relatives take control of children and force them to do sexual activities that are recorded on camera (Dedase-Escoton, et al., 2020, p. 18). When parents are not directly involved, the abuse may be carried out by other people close to children, including family friends, neighbours, or other members of their local community (Terre des Hommes, 2013). Parents who are not actively involved in the crime often overlook and accept their children's involvement in this form of exploitation, as it helps to sustain the family's needs (IJM, 2020; Cruz & Sajo, 2015). A study conducted by the National Center for Missing and Exploited Children (NCMEC) regarding Child Sexual Abuse Material (CSAM) revealed that 74% of cases in which both the abuser and child were known involved the distribution or trading of CSAM facilitated by someone from the child's "circle of trust" such as a relative, guardian, or family friend (IJM, 2020, p. 23).

OSEC continues to exist within families due to a flawed belief that it is harmless and acceptable, because no physical touch or sexual intercourse is involved (Kuhlmann & Aurén, 2015; Varrella, 2017). Additionally, in consideration of the traditional Filipino family values of *utang na loob* (a sense of obligation or indebtedness), some parents appeal to their child's moral duty to help provide for the family in order to manipulate them into participating in abusive activities (Dedase-Escoton, et al., 2020, p. 19; Hernandez, et al., 2018; UNICEF, 2016).

Family members or relatives in charge of the abuse may use intimidation or pressure to compel children to bring in other minors and are responsible for connecting with child predators as well as collecting payments through money service businesses (ECPAT France, 2022, p. 21). Research found that family-run trafficking operations typically generate greater profits than individual ones. The payments to children in family-run operations are usually higher than those in individual operations; however, the majority of the money goes to the traffickers (ibid).

2.1.3. Cybersex dens

Cybersex dens are covert operations, largely hidden in poor neighbourhoods, where trafficked or recruited children are forced by facilitators or traffickers to provide sexual activities for OSEC customers (Dedase-Escoton, et al., 2020, p. 18). Children may be targeted by unscrupulous individuals who use the internet and information communication technologies (ICTs) to offer them employment and a way to make quick money (ECPAT France, 2022, p. 21). This activity can be conducted in private residences, as well as in large-scale underground organizations, which are often managed by organized criminal groups, including foreign nationals. The size and complexity of these underground operations can vary, and they can be hidden behind legitimate businesses, such as internet cafés (ibid).

2.2. The demand side of OSEC

An analysis of OSEC customers revealed that they were predominantly male between 40 and 59 years old and from Western countries (Dedase-Escoton, et al., 2020, p. 18). OSEC customers were most commonly recorded to be from the United States, United Kingdom, Australia, and Western European/Nordic nations (IJM, 2020, p. 12). According to Chief Constable Simon Bailey, the National Police Chiefs' Council (NPCC) Lead for Child Protection and Abuse Investigations, UK has been identified as the third biggest consumer of live streamed abuse of children in the world (Jay, Evans, Frank, & Sharpling, 2020, p. 74). An intelligence update from the National Crime Agency (NCA) indicates that there are a minimum of 300,000 individuals residing in the United Kingdom who pose a sexual threat to children online (Grierson & Weale, 2020).

OSEC customers get in touch with facilitators or traffickers to pay to order OSEC materials. For example, the Australian Institute of Criminology conducted a study that found 256 Australians had paid more than $1.3 million over a 13-year period to view live streamed child sexual abuse in the Philippines (Brown, Napier, & Smith, 2020). IJM stated that both demand-side OSEC offenders and supply-side facilitators engage in human trafficking, because OSEC customers engage in the crime through remote and "proxy" means, in collusion with in-person traffickers (ibid). In some instances, the physical trafficker acts as an 'agent' for the demand-side offender, who is the 'main perpetrator'. Both criminals collaborate to make money and generate CSEM for the physical trafficker's financial gain and remote trafficker's sexual gratification (ibid).

2.3. Victims of OSEC

Studies have found that victims of OSEC are generally young children, with a significant proportion being male victims and sibling groups (Terre des Hommes, 2013; Garcia & Manikan, 2014; UNICEF, 2016; Ramiro, et al., 2019). Children are particularly vulnerable to exploitation because they may not have the ability to recognize or report abusive behaviour. Male victims may also be less likely to come forward due to stigma or fear of not being believed. Sibling groups may be targeted because abusers see them as an easy way to gain access to multiple victims at once (Dedase-Escoton, et al., 2020, p. 18).

Poverty, family size, and family structure can all be risk factors for exploitation (Terre des Hommes, 2013). Children from poorer families may be particularly vulnerable to exploitation because they lack access to resources and support that can help protect them from harm (Ramiro, et al., 2019). Children from larger families may also be at increased risk due to a lack of individual attention and supervision (Dedase-Escoton, et al., 2020, p. 19). Broken or unstable families likewise exacerbate vulnerability, because they may not have a consistent source of support and protection (ibid).

Poverty can be a significant contributing factor to OSEC because limited income opportunities and a lack of education and work skills can make it difficult for individuals to support themselves and their families. This may lead people to turn to illegal or risky activities, including exploitation of their children, as a means of survival (Hernandez, et al., 2018; Cruz & Sajo, 2015; Garcia & Manikan, 2014; United Nations Office on Drugs and Crime, 2015). Poverty can also make individuals and families more vulnerable to exploitation by others, who prey on their desperation and lack of resources (Dedase-Escoton, et al., 2020).

Financial motivation is often a key factor in the involvement of traffickers and victims in OSEC. Traffickers may be motivated by the profits they can make from selling access to OSEC, as evidenced by research showing that people who engage in trafficking may see it as a way to make money and meet their own needs (IJM, 2020). IJM's casework data in the Philippines has revealed that out of the more than 250 cases they have worked on, the abuse endured by children at the hands of these offenders typically goes beyond simply displaying erotic behaviour (IJM, 2020, p. 12). Sexual exploitation commonly involves forcible sexual penetration, which is classified as rape in the Philippines and many other jurisdictions. Additionally, minors are oftentimes forced to participate in sexual activities with other children, sexually abused by an adult, and even subjected to other inhumane acts, such as bestiality. Furthermore, the data indicates that over half of the victims are 12 years-old or younger, with over 100 of them being 6 years-old or younger when they were rescued (ibid).

In 2017, the Internet Watch Foundation (IWF) conducted an international analysis of 2,000 images and videos of live streamed sexual abuse of children (Internet Watch Foundation, 2018).The IWF employed a snowball sampling technique, which began by obtaining seed URLs from its historic dataset and through search engines, using keywords identified from the IWF Hotline. All seed URLs were manually reviewed to determine whether they matched the criteria of the study.

Results showed that 98 percent of the victims were 13 years old or younger, and 28 percent were 10 years old or younger. Further, 40 percent of the captures were classified by the IWF as containing serious sexual abuse, including rape and torture of children (ibid).

2.4. Common themes in OSEC literature

A number of studies have been conducted to identify the distinct nature of OSEC. Focusing specifically on OSEC cases in the Philippines, they have found that OSEC cases share the following common themes:

- Consideration of OSEC as a way to make easy money;
- Lack of awareness and knowledge about OSEC;
- Easy access to internet and technology, particularly in the Philippines; and
- Proficiency in English language, particularly in the Philippines.

Sections 2.4.1 – 2.4.4. below briefly explain the most common feature of OSEC cases stemming from the Philippines.

2.4.1. Easy way to earn money

Victimization is a common occurrence in communities that are suffering from extreme poverty or destitution. In many instances, OSEC victims are exploited by their parents and relatives, who are motivated by economic need and push them into OSEC as a source of income due to their irregular or seasonal wages, or lack of a permanent source of livelihood (ECPAT France, 2022, p. 20). Although the monetary rewards from OSEC cases are relatively small, they are much larger than a day or weeks' worth of the Philippine minimum wage, which makes them an attractive proposition for facilitators and traffickers (ibid). According to the World Bank Group, 16.7% of the population of the Philippines was living below the national poverty line in 2018 (The World Bank, n.d.).

Most respondents in Dedase-Escoton et al.'s study on OSEC highlighted poverty and the belief that it is a convenient way to earn money as significant risk factors for engaging in OSEC (Dedase-Escoton, et al., 2020, p. 36). It was reported that a lack of stable income and financial resources made facilitators and victims particularly susceptible to this form of abuse. Respondents stated that families often use poverty and the need to survive as a justification for subjecting their children to live streamed sexual acts (ibid). Additionally, it was pointed out that not all perpetrators are necessarily in a lower economic class, as these individuals may have well-off clients. Some respondents indicated that people may resort to OSEC to finance their 'wants', rather than their needs (ibid).

2.4.2. Lack of awareness and knowledge about OSEC

There is a widespread lack of recognition that live streamed sexual exploitation is a criminal offense, as well as a misconception that it does not cause any harm to the victims. Family and community members often mistakenly think of live streamed sexual exploitation as a harmless practice, given that no physical contact or sexual intercourse takes place (although this is not always the case).

One respondent in the Dedase-Escoton et al. study articulated that ‘they have a no touch, no harm attitude’ (2020). Other respondents indicated that the rationale often used to justify the perpetration of OSEC was that ‘it’s just a show’, ‘it’s just a picture’, and ‘they have nothing to lose’ (ibid).

The majority of respondents in the Dedase-Escoton et al. study highlighted the lack of knowledge and awareness regarding online sexual exploitation of children as another key factor in its enduring proliferation in families and communities (2020, p. 37). It is reported that both offenders and victims were unaware that this kind of abuse is a crime punishable by law. Most non-offending family members surveyed had no idea what OSEC is. Some participants believed that increasing awareness of this being a criminal offence within families and communities could be beneficial, as it could encourage reporting of suspected cases to the authorities and facilitate prevention measures to combat this form of abuse (ibid). Further, raising awareness of the potential consequences of OSEC could help deter potential perpetrators, encourage victims to seek help, and inform families about the various forms of online exploitation (ibid).

2.4.3. Access to internet and technology

Research suggests that the affordability and availability of internet and technology are major contributors to the rising number of OSEC cases in the Philippines (Terre des Hommes, 2013; IJM, 2020). Respondents in the Dedase-Escoton et al. study indicated that cell phones are a necessity for Filipinos and are often the first priority when allocating money for goods and services (2020, p. 38). Owning a phone has become increasingly affordable and the internet is widely accessible (ibid). Further, the lack of individual mobile phones or computers is not a hindrance to accessing the web, as there are numerous Internet Cafes and Piso/Peso Nets available (Hernandez, et al., 2018; UNICEF, 2016; Varrella, 2017).

2.4.4. Proficiency in English language

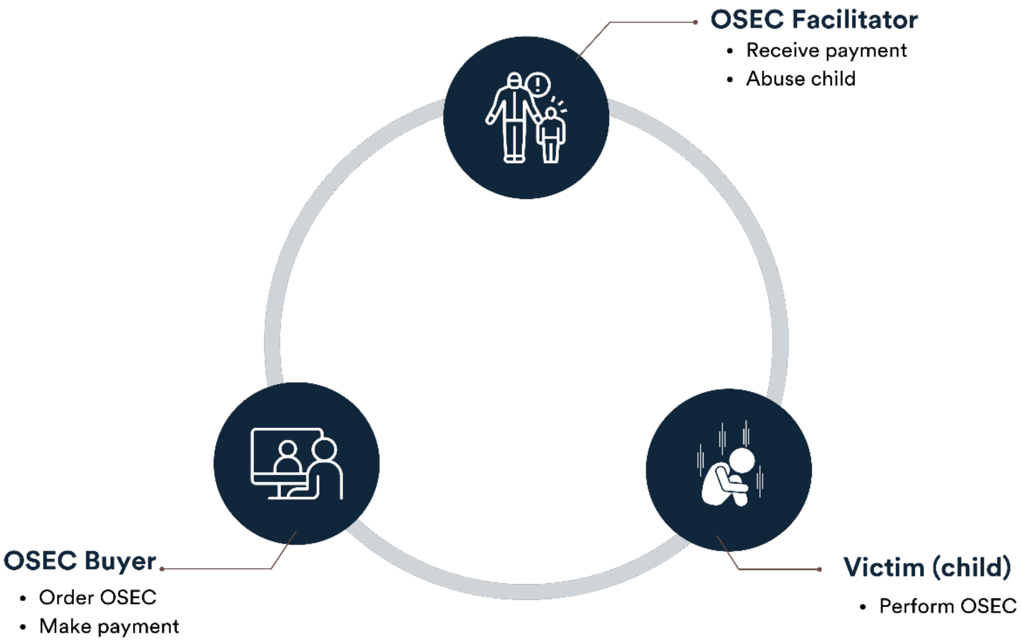
Filipinos’ fluency in the English language is a contributing factor to their access to Western audiences through the internet and technology, thus increasing the risk of engaging in foreign transactions (Hernandez, et al., 2018; IJM, 2020; Ramiro, et al., 2019; UNICEF, 2016; Varrella, 2017). Their facility with the language allows them to communicate, transact, and negotiate with individuals from other countries, particularly those in the West (Dedase-Escoton, et al., 2020). Due to the lack of linguistic barriers, foreigners have the ability to exercise considerable control over both traffickers and victims (IJM, 2020).

The economic situation of facilitators and victims, combined with a desire to gain easy money and a lack of awareness of the issue of OSEC, creates the ideal conditions for this form of abuse to occur. Mobile phones, laptops, internet access, and proficiency in the English language are all exploited as resources to engage in this kind of abuse. In addition, affordability and accessibility made them attractive targets for abusers. This combination of factors creates an environment that facilitates OSEC (Dedase-Escoton, et al., 2020).

3. Facilitation of OSEC

Individuals seeking out child sexual abuse online will often look for traffickers on the surface web, rather than the dark web, searching for people who display characteristics of a typical trafficker, such as someone from a specific geographic region who posts suggestive photos of children and uses flirtatious language (Draper, 2022, p. 17). If the response from the possible trafficker is favourable, they will then start engaging in a dialogue meant to establish trust, often moving to encrypted messaging apps. This leads to the negotiation of a financial transaction for different levels of abuse or exploitation (ibid).

Figure 1: How OSEC is facilitated



In OSEC cases, facilitators often play a large role in ensuring the smooth running of the operation. This can involve coercive and forceful methods, or otherwise convincing children to take part in sexual activities, as well as providing logistical assistance such as finding venues to hold the activities, obtaining and using electronic devices, and setting up payment methods (ECPAT France, 2022, p. 22). Facilitators may be in contact with child sex offenders, instructing children on how to act, providing them with clothes to entice more child sex offenders, and desensitizing them to sexual content by exposing them to pornographic material (ibid). They may also record the sexual abuse of child victims and distribute it online.

OSEC, and particularly live online child sexual abuse, is a devastating form of abuse that involves two distinct elements. Firstly, the child is coerced to take part in sexual activities, alone or with someone else, which already constitutes a form of sexual abuse (Draper, 2022, p. 12). Secondly, the sexual activity is broadcast live through information and communication technologies (ICTs), and watched by someone else, often the person who requested or ordered the abuse (ibid). In some cases, this has been set up as an actual business to make money off the exploitation (IJM, 2020). The Luxembourg Guidelines note that this form of abuse is not new, but the element that is new is the fact that the perpetrator can be in a different country than the victim (ECPAT International, 2016). This makes the crime even more serious and difficult to prosecute, as it means that the perpetrator is likely beyond the reach of the law. Further, it makes it more difficult to locate the victim, as well as to provide them with the necessary support and help they need.

The Australian Institute of Criminology conducted a comprehensive study to investigate cases of live online child sexual abuse and determined that facilitators were involved in 51 out of the 145 cases (Napier, Teunissen, & Boxall, 2021). The number of facilitators in contact with the child sex offenders varied from one to eight, and the number of offences committed by each facilitator fluctuated from one to fourteen (ibid). This indicates that some facilitators were involved in multiple cases of abuse, while others were involved in only one.

Additionally, more than half of child victims (51%) had a facilitator arrange their sexual abuse; the facilitator was often used by the child sex offender to establish contact with the child victim (ibid). Meanwhile, the remaining child victims (49%) communicated directly with the child sex offenders without the involvement of a facilitator. (Ibid).

In a research study conducted by the International Justice Mission (IJM) examining 141 facilitators identified by law enforcement in the Philippines, the majority of facilitators were female (66%) and had a median age of 27 years (IJM, 2020). In the 71 cases of sexual abuse investigated by law enforcement, these facilitators were predominantly direct relatives of the child victims—41% being biological parents and 42% being other family members (ibid). This data suggests that the majority of facilitators of child sexual abuse in the Philippines are female and are typically direct relatives of the victims.

Similarly, the Australian Institute of Criminology found that out of 20 facilitators, 15 were female and their ages ranged from 16 to 35 years (Napier, Teunissen, & Boxall, 2021). The median age for 12 of these facilitators was 20 years, indicating that the majority of facilitators were young women between the ages of 16 and 35 (ibid). This suggests that there is a trend of young women taking on the role of facilitator. There is a need for further research into the reasons why this is the case.

3.1. Live streamed sexual exploitation of children

Live streamed sexual exploitation of children is different from other forms of CSAM shared on the internet due to its ‘real-time’ element (Açar, 2017; Europol, 2019). This means that the abuser can request the child to be sexually abused either before or during the live streaming session, and the child is subjected to the abuse while the live stream is happening (ECPAT International, 2017). This is in contrast to other types of CSAM which are typically pre-recorded and released or shared after the abuse has already occurred (Açar, 2017). The immediacy of the live stream means that the abuser can gain gratification from the real-time reaction of the child, and the abuser can also receive instructions from other viewers who can also gain gratification from the abuse. Live streamed sexual exploitation of children involves the real-time transmission of audio and video files over a wired or wireless internet connection. This means that the data is sent instantly to the electronic device of the viewer, allowing them to remotely witness and participate in the abuse taking place (IJM, 2020).

Unlike with other forms of digital media, this type of streaming does not leave any trace on the electronic device, as no files are downloaded and stored onto its hard disk (ECPAT France, 2022, p. 9). As soon as the streaming is stopped, the material is gone, making it only available one time and leaving no trace unless it is deliberately recorded (ibid).

According to media reports, child sexual abuse was being live streamed in the Philippines as early as 2008 (de Leon, 2013). The availability of live video streaming platforms (and adult webcam sex shows) to the public since the early 2000s likely meant that this abhorrent activity was taking place even earlier than this (Brown, Napier, & Smith, 2020, p. 2). INTERPOL has observed a significant increase in the live streaming of child sexual exploitation for money in recent years, an issue which is of grave concern (INTERPOL, 2020). The WePROTECT Global Alliance has estimated that live streaming will account for 13% of all internet video traffic by 2021, indicating the scale of the problem (WeProtect Global Alliance, 2018, p. 8). The National Crime Agency (NCA) has identified live streamed child sexual abuse as ‘one of the emerging threats’ to children in the present day (Independent Inquiry Child Sexual Abuse, 2020, p. 74).

As explained above, live streamed sexual exploitation of children often facilitated by a relative or known adult in the victim’s home, has no boundary, with affluent perpetrators in high-income countries paying large sums of money for brief, on-demand abuse incidents that occur in lower-income countries. The issue has been extensively studied in Southeast Asia, however it is now extending to other regions (Davy, 2017). It is extremely difficult to accurately measure the ever-growing magnitude of the problem due to the challenges in detecting the faint and transient digital footprints that live streamed abuse leaves behind (Bracket Foundation, 2019).

Live online child sexual abuse involves the participation of a child in sexual activity, alone or with other children or adults, that is transmitted live to viewers over the internet (ECPAT France, 2022, p. 8). The child may be coerced or forced into participating by an adult or trafficker who is manipulating the sexual activity. This abuse can be viewed remotely by people in any part of the world. In many cases, the demand-side child sex offender requests and/or directs the abuse, or the trafficker/facilitator profits from it (ibid). There is no physical contact between the demand-side abuser and the victim; instead, victims are subjected to a form of psychological manipulation as their abusers watch and direct the activity for their own gratification (ibid).

3.2. The prevalence of OSEC

It is challenging to calculate the global scale of child sexual abuse and exploitation online with accuracy due to the discrepancies in definitions and data collection practices among different jurisdictions. Contrary to what many people think, most child sexual abuse material (CSAM) can be found on the open web, not just in hidden areas. The US-based National Center for Missing and Exploited Children (NCMEC) gathers data on CSAM and the exchanging of such content that has been identified by web companies based in the US. In 2022, NCMEC received a total of over 31.9 million reports of suspected child sexual exploitation (NCMEC 2023), representing a significant growth from 21.7 million reports in 2020, and more than ten times the number of cases reported a decade prior (NCMEC, 2022).[2] This demonstrates the urgent need to confront this issue and the importance of establishing better data collection mechanisms to ensure reliable and accurate reporting.

The majority of reports (21.4 million) collected by NCMEC come from large tech companies such as Facebook (now known as Meta). During the period between April and September 2021, Meta, incorporating Facebook, Instagram, and WhatsApp, took action to address 46.5 million pieces of content which they suspected to be related to child sexual exploitation (Skidmore, Aitkenhead, & Muir, 2022, p. 15). In addition, these companies use automated search algorithms to proactively seek out this type of material.

In 2017, the Canadian Centre for Child Protection initiated Project Arachnid—a web crawler designed to use photoDNA to spot known records of CSAM. In addition, it was commanded to look for probable forums and chat rooms.[3] Over two years, this system managed to identify 7.4 million potential CSAM files, resulting in 1.6 million take down notices dispatched to US and Canadian host sites, or referred to INHOPE (The National Archives, n.d.). This data shows that the production and viewing of CSAM is occurring at a high frequency.

[2] The National Center for Missing and Exploited Children (NCMEC) administers the CyberTipline, a platform for members of the public and electronic service providers to inform authorities about any possible incidents of child sexual abuse that they suspect. First established in 1998, the CyberTipline has since been the recipient of over 116 million reports.

[3] PhotoDNA was originally developed by Microsoft and Dartmouth in partnership with NCMEC to enable online service providers to better detect child exploitation materials. PhotoDNA creates a unique digital signature (known as a "hash") of an image which is then compared against signatures (hashes) of other photos to find copies of the same image. When matched with a database containing hashes of previously identified illegal images, PhotoDNA is an incredible tool to help detect, disrupt and report the distribution of child exploitation material. (Microsoft, n.d.)

Over the past decade, there has been an explosive growth in the amount of CSAM available online. According to statistics from NCME:

> **"…the number of images and videos of suspected child sexual abuse jumped from 450,000 in 2004 to a staggering 44 million files in 2021."**
>
> **- (NCMEC, 2022; Bracket Foundation, 2019, p. 6).**

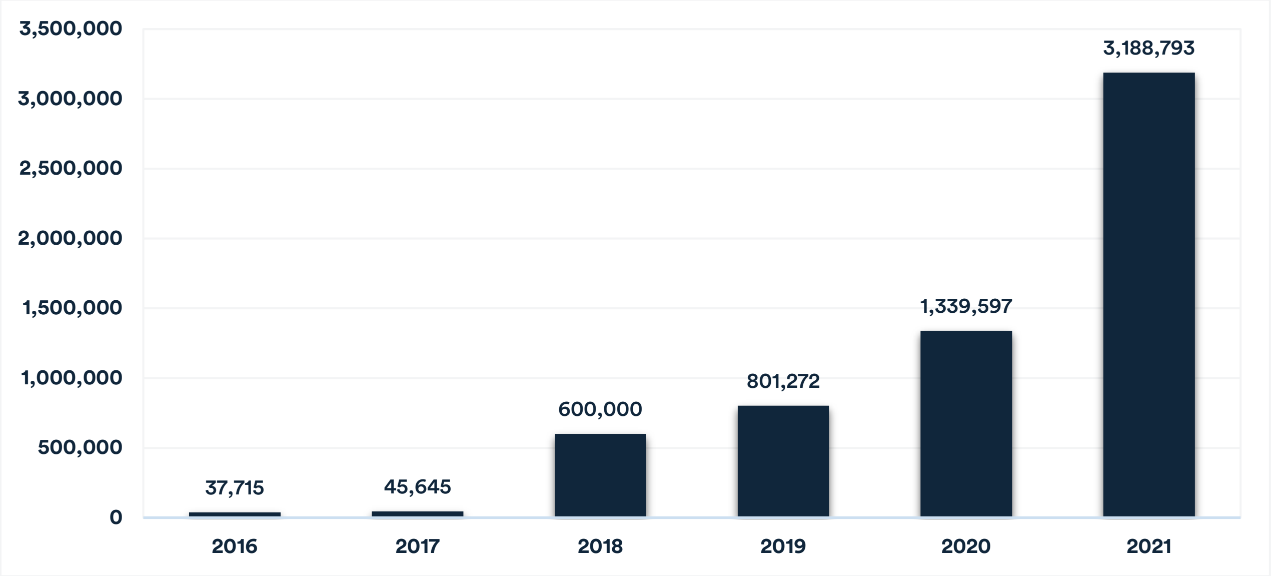
Similarly, there has been a drastic increase in the number of URLs containing CSAM. In 1998, only 3,000 such URLs were detected, but by 2019 there were 18.4 million such URLs reported (Bracket Foundation, 2019, p. 6). This drastic increase in the amount of CSAM available online is deeply concerning and indicates the gravity of the issue of child exploitation.

The Internet Watch Foundation (IWF), an organization in the UK, has likewise reported a tremendous surge in the number of URLs containing CSAM. In 2021, they detected 252,194 URLs, which marks a 707% rise since 2014 when there were only 31,266 URLs (Internet Watch Foundation, 2021). However, it should be noted that the increased detection of CSAM is due to advancements in technology, rather than being entirely a function of increased prevalence. Only a small proportion of the sites hosting CSAM were located in the UK (0.15%), while the Netherlands had the largest proportion (41%) (ibid).

In 2013, an extensive study conducted by the international charitable organization, Terre des Hommes, was conducted to explore the prevalence of OSEC (Terre des Hommes, 2013). The study spanned a period of 10 weeks and involved researchers assuming the role of young Filipino girls in 19 public chat rooms on the Internet. During the period of research, it was discovered that there was an alarming number of predators from a multitude of countries around the world who sought to initiate sexual interactions with the researchers. Ultimately, the research identified over 20,000 predators as having shown interest in the researchers posing as Filipino children (ibid).

OSEC is a rapidly rising global concern, particularly in the Philippines, which has been labelled as the 'global hotspot' or 'global epicentre' for OSEC cases (IJM, 2020; Brown, 2016). This situation has been further compounded by the Philippines being one of the top ten countries producing child sexual exploitation material (CSEM) (Dedase-Escoton, et al., 2020, p. 11). ECPAT highlighted that law enforcement agencies worldwide report that the majority of children subjected to live streamed sexual exploitation online are situated in South-East Asia, particularly in the Philippines (Simantiri, 2017).

Figure 2: NCMEC CyberTipline reports regarding the Philippines



NCMEC's reports found that the Philippines had experienced an unprecedented rise in the number of CyberTipline reports on online child exploitation in recent years (NCMEC, 2021; NCMEC, 2020; NCMEC, 2019; Dedase-Escoton, et al., 2020, p. 17). In 2016, 37,715 such reports were received, while in 2017 this figure had risen to 45,645. The number of reports continued to increase in 2018 with 600,000 reports, 801,272 reports in 2019 and 1,339,597 reports in 2020. However, 2021 saw an extraordinary spike in the number of reports, with 3,188,793 reports being received, which represented a staggering increase of almost three times the 2020 figure and over 84 times the 2016 figure. Online child sexual abuse is becoming an increasingly serious issue as technological infrastructure and hosting services become more accessible and cost effective.

Nearly all of the world's CSAM is located in Europe and North America, with the Netherlands alone accounting for 47% (Bracket Foundation, 2019, p. 6). Further, the supply-side component of OSEC is spreading quickly to developing markets as they gain access to modern technology and the internet. This enables them to easily access and share CSAM, which can be further distributed to a larger audience (ibid). This has the potential to create a dangerous environment for children in an increasingly wide pool of countries, as they become more vulnerable to exploitation by traffickers and perpetrators.

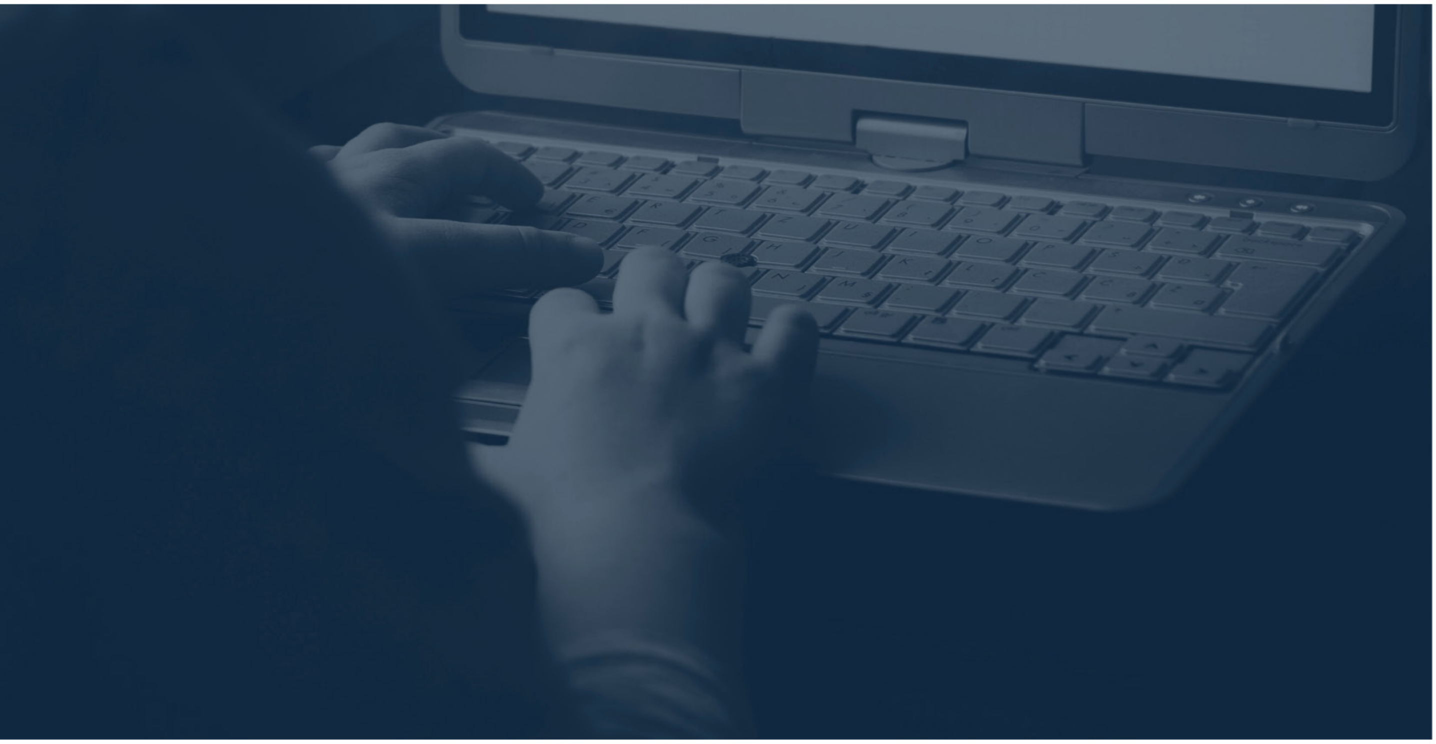
Recent studies have revealed a significant rise in the demand for live online child sexual exploitation over the past few years, with a notable surge occurring in the wake of the Covid-19 crisis. According to Europol, the Philippines was one of the nations to experience a particularly severe rise in live online child sexual exploitation cases during the pandemic, due to the combined effect of the lockdown on already impoverished families, whose limited sources of income were further reduced, and the absence of children from school (Europol, 2020).

Other studies also found an increase in online child sexual abuse during the Covid-19 pandemic. For example, in September 2020, INTERPOL released a statement warning that the need for streaming child sexual abuse was expected to increase due to the continued restrictions on travel - (INTERPOL, 2020).

According to Europol, in March 2020, there was a noticeable growth in the amount of child sexual exploitation materials (CSEM) downloaded in Spain and there were attempts to access CSEM websites in Denmark (Europol, 2020, p. 7).

The Internet watch Foundation (IWF) documented a dramatic increase in the number of attempts to view child sexual abuse material by internet users in the UK during the Covid-19 lockdown, with at least 8.8 million attempts to access videos and images of children suffering sexual abuse (Internet Watch Foundation, 2020). The eSafety Commissioner, Australia's national independent regulator for online safety, likewise reported a dramatic 86% increase in reported cases of image-based abuse over the three weeks prior to April 9, 2020 (Medora, 2020).

The Australian Federal Police (AFP) and the Australian Center to Counter Child Exploitation (ACCCE) noted the emergence of child abuse forums in the wake of the Covid-19 stay-at-home measures (Australian Federal Police, 2020). Further, it was reported that child sexual abuse websites were overwhelmed due to the rise in internet traffic. During the months of April, May, and June 2020, the ACCCE observed a 122% spike in reports in comparison to the previous year (ibid).



4. The financial dimension of OSEC

Europol and the Australian Transaction Reports and Analysis Centre (AUSTRAC) both agree that the live streaming of child sexual abuse is primarily motivated by financial gain (AUSTRAC, 2019; Europol, 2019). Similarly, the Republic of the Philippines Anti-Money Laundering Council (AMLC) also highlights that OSEC, including live streaming, includes a financial motivation since facilitators want to make financial gains out of OSEC- (AMLC, 2020a, p. 14).

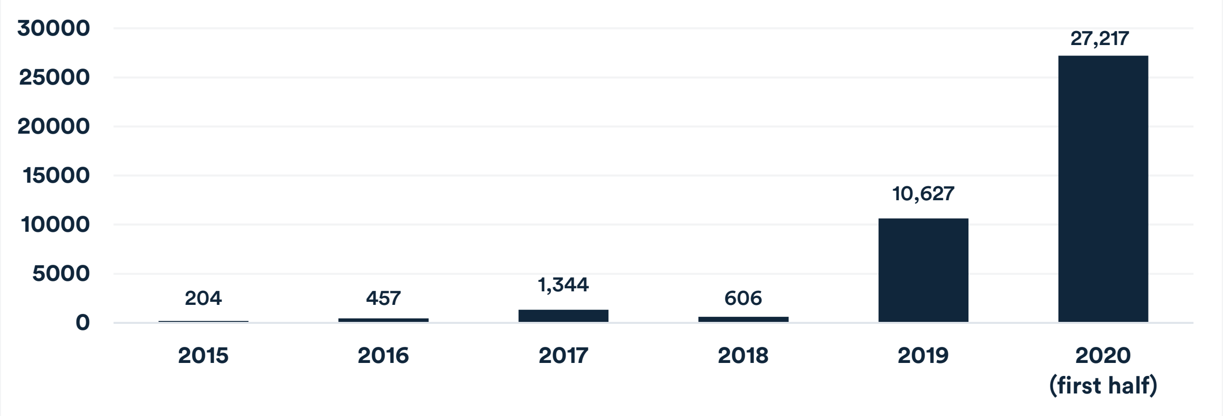
Typically, viewers of live streamed OSEC pay an amount to the facilitators or, in rare cases, the children directly. This payment can be made through a variety of methods, such as money transfer services, direct deposit into a bank account, or with virtual currency exchange (Varrella, 2017, p. 49).

Studies have observed that the cost of live streamed OSEC in the Philippines is typically inexpensive, because of the poverty experienced by those involved in supplying the service (Masri, 2015). The affordability of live streamed OSEC is a major draw for sexual predators residing in developed countries, as it allows them to satisfy their desires without having to take the risk of physically sexually abusing a child (Brown, Napier, & Smith, 2020, p. 3).[4]

The AMLC worked to identify OSEC related suspicious transaction reports (STRs) to address the financial dimension of this crime in the Philippines. It reported an increasing trend in the OSEC related STRs between 2015 and 2020, finding a total of more than 40,000 STRs associated with OSEC in this period (See Figure 3). AMLC attributed the dramatic increase in STRs to the rising awareness of the financial sector related to reporting suspicious transactions—fostered through various awareness campaigns conducted by AMLC, law enforcement agencies, and private organizations (AMLC, 2020a, p. 11).

[4] It should be noted that Europol has raised the alarm that live streaming of OSEC can present a risk of offenders travelling to perpetrate abuse in person, as some offenders try to make contact with children seen in a live streaming session (Europol, 2016).

Figure 3: Volume of STRs associated with OSEC in the Philippines[5]



AMLC also reported on the total value represented by STRs related to OSEC. Table 1 below shows the total volume of STRs associated with OSEC (or child pornography) in the Philippines. A total of ₱192,008,106.14 Philippine Pesos (PHP) ($3,527,194.67 USD) was spent on OSEC or child pornography between 2015 and June 2020 (AMLC, 2020b).

Table 1: Total value of STRs associated with OSEC in the Philippines

Year	Total Number STRs	Total Amount (PHP)
2015	204	1,414,134.09
2016	457	4,120,715.00
2017	1,344	6,923,425.18
2018	606	659,090.05
2019	10,627	65,807,685.16
2020	27,217	113,083,056.66
Total	**40,455**	**192,008,106.14**

The cost for a single OSEC show varies depending on its duration, the number and age of the children involved, and the sexual acts they are forced to perform (ECPAT France, 2022, p. 23). The amount charged for such shows typically ranges between ₱500 and ₱2000 PHP, equivalent to $9 to $36 USD (Varrella, 2017, p. 49). NGOs working on OSEC in Philippines have likewise noted that the typical cost for live streaming of an OSEC session usually ranged from ₱500 to ₱2,000 PHP (European Financial Coalition, 2015). Other studies have indicated that the amount paid per session can range from $30 to $3,000 USD (Desara, 2019, p. 32). These findings are in line with the findings of the AMLC, reporting that OSEC involves a foreign remitter paying a small amount of money (usually $200 USD or below) to facilitators in the Philippines (AMLC, 2020, p. 15).

[5] It should be noted that AMLC published two reports on STRs. Although one report refers to 'STRs asscoiated with child pornography', the other report refers to 'STRs associated with OSEC'. However, the figure in the both reports are the same in terms of OSEC related STRs and child pornography relates STRs. It appears therefore that AMLC uses both term interchangeably. (AMLC, 2020a); (AMLC, 2020b)

Figure 4: Range of payment amounts per OSEC transaction between 2015 and 01 June 2020 (in PHP)

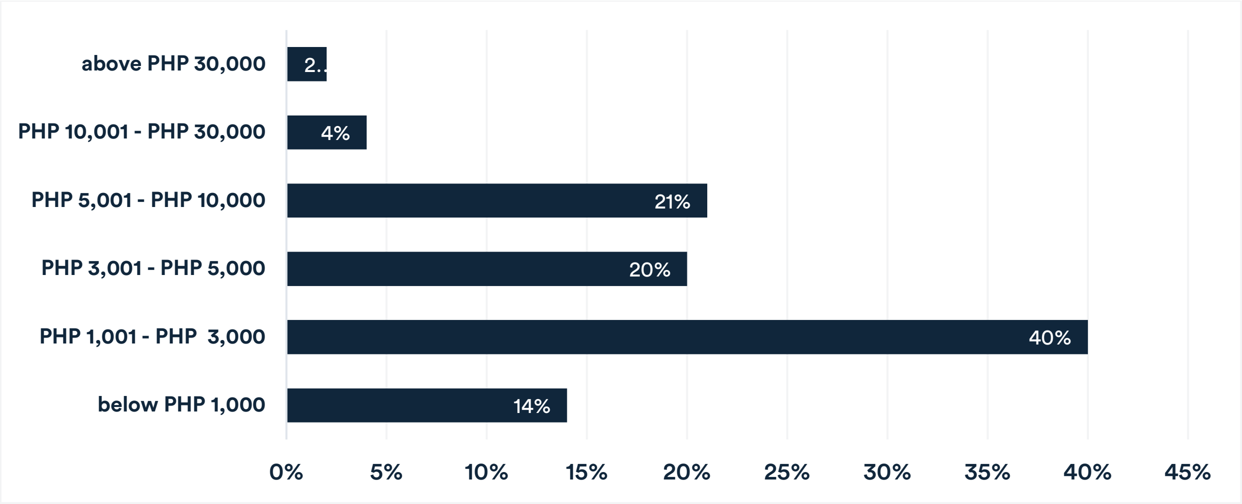


Figure 4 summarizes AMLC data on the amount of funds per transaction associated with OSEC in the Philippines for the period from 2015 to June 2020. This shows that 81% of transactions made for OSEC were between ₱1,000 PHP ($18.37 USD) and ₱10,000 PHP ($183.70 USD) (AMLC, 2020, p. 15).

Text box 1: AUSTRAC data on financial transactions associated with OSEC in the Philippines

A comprehensive study of *AUSTRAC* data regarding financial transactions made by consumers of live streamed OSEC found that *256 individuals made 8,994 overseas transactions*, with *2,714 (30%)* being directed to known OSEC facilitators in the Philippines (Brown, Napier, & Smith, 2020). Notably, eight of the demand-side perpetrators (3%) were found to have made a total of *1,365 transactions* to the Filipino facilitators, accounting for 50% (n=1,365) of the total financial transactions to OSEC facilitators in the Philippines. The number of transactions per person among these eight demand-side perpetrators was found to range from 77 to 479. Meanwhile, 25% of demand-side perpetrators (n=64) made up a small portion of transactions, with almost half (48%, n=122) only buying one CSEM item from the identified facilitators - (ibid).

The total value of the 2,714 payments made to live streaming facilitators was $1.32 million Australian Dollars (AUD) (approximately $870,500 USD), with an average payment of $488 AUD ($320 USD). This average figure is higher than usual due to a few large transactions; 193 (7%) payments were worth $1,000 or more. In contrast, the median payment value was much lower, at $78 AUD ($51 USD) and 25% of the transactions (n=679) were valued at $36 AUD ($24 USD) or less. Three-quarters (n=2,036) of the payments were worth $170 or less (ibid).

The authors also observed a substantial increase in the frequency and magnitude of transactions. Of the 256 individuals who made a financial transaction, 134 made a second transaction, with 12 of these individuals making over 50 payments. The number of separate transactions made by those making over 50 payments ranged from 55 to 479 separate transactions each, indicating a significant escalation in their spending - (ibid).

4.1. Payment platforms used for OSEC

The AMLC has noted that different payment platforms are being used to facilitate OSEC. They found that the majority of STRs related to OSEC or child pornography in the Philippines were made via money service businesses (MSBs).[6] Money service businesses (MSBs) are businesses that transmit or convert money—this includes both banks and non-bank financial institutions.[7] Table 2 shows that MSBs are the most frequently used payment method to transfer funds for OSEC (AMLC, 2020, p. 5); the vast majority of OSEC buyers send money via MSBs, and these payments are received by facilitators through the same platform.

Table 2: Frequency of different payment platforms for OSEC in the Philippines

Payment Methods	Number of STRs (2015 to 2018)	Percentage	Number of STRs (2019 to June 2020)	Percentage
Money Service Businesses	1,548	59.29%	36,831	97.32%
Electronic Money Issuer	0	0	512	1.35%
Banks	920	35.24%	444	1.17%
Virtual Currency Exchanges	24	0.92%	57	0.15%
Insurance Companies	1	0.04%	0	0.00%
Stock Savings & Loan Associations	118	4.52%	0	0.00%

MSBs are one of the most frequently cited sources of payments for OSEC by law enforcement (European Financial Coalition, 2015). However, it is difficult to accurately estimate the extent of their misuse due to the nature of the transactions, which tend to be of low value (usually less than $100 USD) and are often sent by individuals with no family ties to the receivers (Brown, Napier, & Smith, 2020, p. 3). These payments are made on an intermittent basis, typically once or twice a week, and are mainly sent from developed countries to those in South East Asia.

This pattern of low-value transactions is also common with other types of funding, including charity payments, making it even more difficult to detect and identify the misuse of money transfer services (European Financial Coalition, 2015).

[6] Note: one of the AMLC's two reports published in 2020 refer to OSEC, while the other report refers to child pornography. However, both reports provide the same figures in terms of STRs; the AMLC uses OSEC and child pornography interchangeably.

[7] The scope of the term MSB can vary in different jurisdictions. For example, in the UK this includes any business that transmits money or representatives of money, provides foreign currency exchange such as Bureaux de change, or cashes cheques or other money related instruments (Financial Conduct Authority, n.d.). In the US, MSBs can be any person or entity doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: currency dealer or exchanger; check casher; issuer of traveller's checks, money orders or stored value; seller or redeemer of traveller's checks; money orders or stored value; money transmitter; and U.S. Postal Service (FINCEN, n.d.).

The primary reason for the high reliance on MSBs in transferring money for OSEC is explained by the AMLC (2020a, p. 17) as follows:

- MSBs are not controlled or regulated as stringently as banks. Banks' policy of 'know-your-customer' can have a deterrent effect on criminals because they want to avoid strict measures.
- The accessibility of MSBs in most areas in the Philippines is considered another reason for much higher reliance on this payment platform compared to banks and other payment methods.

In the context of the Philippines, well-established money transfer services are a contributing factor to financial flows for OSEC. For example, participants in the Disrupting Harm study highlighted the pre-existing money transaction systems in the Philippines were a major enabler of OSEC (ECPAT, INTERPOL and UNICEF, 2022, p. 75). The dense network of money transfer services, established to support remittances sent by Filipino migrant workers, has made payments for illicit content—such as sexual images or videos and access to live streaming of OSEC—significantly easier (ibid).

The Philippines has established a highly developed MSB and Fintech infrastructure due to the large number of Filipinos living and working abroad who use MSBs to provide financial assistance to their relatives in the Philippines (ECPAT France, 2022, p. 20). This is largely attributed to the progression of technology, which has allowed for increased accessibility and affordability of remittances. According to the World Bank Group, the Philippines was one of the leading recipients of remittances in the East Asia and Pacific region in 2020, representing a total of $34.9 billion USD (The World Bank, n.d.). Additionally, remittance fees to the Philippines are among the lowest in the East Asia and Pacific region, making it an attractive option for those sending money (Global Knowledge Partnership on Migration and Development, 2021). MSBs in the Philippines commonly use the Filipino word 'padala' which translates to relay, remit, send, or transmit (ECPAT France, 2022, p. 20). This highlights the importance of remittances to the Filipino people, as it provides them with a necessary means of support.

Studies found that the most common way of transferring payment for live streaming of OSEC is through the classic Western Union money-transfer system (Terre des Hommes, 2013). For example, National Bureau of Investigation Anti Human Trafficking Division (NBI-AHTRAD) records for the two-year period spanning 2017 to 2018 revealed that Western Union was the most frequently utilized service, with a reported total of 12 incidents (ECPAT, INTERPOL and UNICEF, 2022, p. 75). This was followed by Smart Money Padala, which had two reported incidents, and PayPal and Cebuana Lhuiller, each of which had one incident reported (ibid).

Many OSEC customers choose to use PayPal instead since they can set up accounts under a false name and thus protect their anonymity (Desara, 2019, p. 25). However, some OSEC customers were found not to be concerned about being exposed to any potential risks because amounts transferred for a single performance are usually relatively small, making them confident that their activities will not be noticed by law enforcement agencies (ibid).

Mobile phone-based prepaid payment applications, including Smart Padala, are also reportedly being used to transact payments for OSEC in the Philippines (ECPAT, INTERPOL and UNICEF, 2022, p. 75). These applications only require a mobile phone and a Padala number for access, and do not necessitate the presentation of any form of identification (ibid).

Table 3 shows the volume of remittances related to OSEC made via different payment platforms in the Philippines between 2015 and June 2020 (AMLC, 2020b). This shows that the vast majority of financial flows in OSEC cases has been made via MSBs. MSBs represented 89.42% (PHP 159,967,903.84 or $2,937,616.99 USD) of the total amount of money used to facilitate OSEC between 2019 and June 2020, compared to 6.92% through Electronic Money Issuers (EMIs) and 3.63% in Banks (AMLC, 2020b, p.5)

Table 3: Volume of remittances related to OSEC by different payment platforms

Payment Methods	Total Amount (PHP) (2015 to 2018)	Percentage	Total Amount (PHP) (2019 to June 2020)	Percentage
Money Service Businesses	10,243,138.00	78.09%	159,967,903.84	89.42%
Electronic Money Issuer	0.00	0.00%	12,381,074.45	6.92%
Banks	2,270,185.00	17.31%	6,487,293.53	3.63%
Virtual Currency Exchanges	230,350.00	1.76%	54,470.00	0.03%
Insurance Companies	0.00	0.00%	0.00	0.00%
Stock Savings & Loan Associations	373,692.00	2.85%	0.00	0.00%

Table 2 and Table 3 demonstrate that offenders and facilitators involved in OSEC transactions usually prefer to use the traditional payment methods such as MSBs and banks, accounting for 98.49% of transactions and 93.05% of the monetary value (AMLC, 2020b).

The AMLC also found that Electronic Money Issuers (EMIs) were employed to move funds for OSEC and child pornography. 512 unique STRs initiated by EMIs were identified between 2019 and June 2020 (AMLC, 2020b, p. 5). EMIs issue electronic money, which is a digital form of currency that can be used to make purchases online or in-person (Financial Conduct Authority, n.d.).

This type of money is often stored in an e-wallet and can be used for transactions. EMIs offer consumers the capacity to electronically store money in convenient payment instruments, which can be used to buy goods and services, send or remit funds, or withdraw money. These e-money instruments include cash cards, electronic wallets (e-wallets) accessible through a mobile phone or other access device, stored value cards, and other similar products (ICAEW, n.d.). Virtual currency has also been used to facilitate OSEC or child pornography in the Philippines.[8] The AMLC reported an increase in the use of virtual currency for OSEC from 24 STRs between 2015 and 2018 to 57 STRs between 2019 and 2020 (AMLC, 2020, p.6).

However, offenders and facilitators of OSEC do not generally rely on virtual currency, compared to other payment methods such as MSBs and bank transfers. This is because offenders—who are usually over 50 years old—may find it more difficult to adapt to the use of new technologies. The lack of access to modern technology due to poverty in the region is another factor impacting the restricted use of EMIs and virtual currency for OSEC in the Philippines (ibid).

[8] AMLC defines virtual currency as a type of digital currency that is generated by a group of individuals online and is typically exchanged online and stored in e-wallets. It is not backed by central banks or government authorities and can only be transferred among the users within the community. It serves as a medium of exchange that can be used to purchase virtual goods or actual merchandise from online vendors who accept it as payment. AMLC also notes that virtual currency can be converted to or from fiat money (AMLC, 2020, p.6).

The use of bank transfers as a method of payment for the purchase of OSEC remains a serious concern. For example, the Australian Transaction Reports and Analysis Centre (AUSTRAC) initiated a legal action against Westpac Banking Corporation, known simply as 'Westpac'—an Australian multinational banking and financial services company (Brown, Napier, & Smith, 2020, p. 3).[9] Westpac was accused of failing to meet its obligations under anti-money laundering and counter-terror finance laws, as well as allowing money transfers to the Philippines suspected to be for child sexual exploitation (Butler, What is Westpac accused of, and how is this related to child exploitation? – explainer, 2019). AUSTRAC identified twelve Westpac customers suspected of paying to OSEC facilitators in the Philippines. These twelve Westpac customers made a total of 3,057 transactions totalling $497,612.20 AUD.

Table 4: Details of twelve Westpac customers suspected of transferring money to OSEC facilitators in the Philippines[10]

Customers	Total Amount in AUD	No. of Transactions	Time Period	Note
Customer 1	$136,000.00	625	November 2013 - July 2019	Traveled to the Philippines in 2014 and 2016; transferred money to a person later arrested for child trafficking and offering children for sexual abuse
Customer 2	$43,000.00	991	November 2013 - June 2019	None
Customer 3	$20,000.00	111	April 2016 - July 2019	Transferred money to a suspected child exploitation facilitator
Customer 4	$52,000.00	340	November 2016 - September 2019	None
Customer 5	$75,000.00	225	June 2015 - August 2019	Traveled to Southeast Asia multiple times from 2013
Customer 6	$32,000.00	209	May 2016 - August 2019	Traveled to the Philippines in 2015/16 and 2017
Customer 7	$62,000.00	207	March 2016 - July 2019	Traveled to the Philippines in 2015, 2017 and 2018
Customer 8	$33,000.00	150	May 2016 - August 2019	Traveled to the Philippines in 2016, 2017 and 2018
Customer 9	$24,000.00	81	March 2018 - July 2019	None
Customer 10	$13,000.00	73	March 2017 - February 2019	Traveled to the Philippines in 2017 and 2019
Customer 11	$5,000.00	35	February 2019 - August 2019	None
Customer 12	$2,612.20	10	June 2019 - August 2019	Had a prior conviction for child exploitation offences
Total	$497,612.20	3,057		

[9] AUSTRAC is responsible for preventing, detecting and responding to criminal abuse of the financial system to protect the community from serious and organised crime (See: https://www.austrac.gov.au/).

[10] (Butler, Legal breaches allowed Westpac customers to pay for child sexual abuse undetected, Austrac alleges, 2019).

4.2. Common indicators of financial transactions for OSEC

AUSTRAC has found different payment platforms being used by OSEC customers and facilitators to transfer payments (AUSTRAC, 2022). The most common payment methods include remittance service providers, bank transfers, digital wallets and mobile money, digital currency, prepaid debit or credit cards, global phone recharge top-ups and online payment applications (ibid). OSEC customers often utilize seemingly harmless payment descriptions (such as 'accommodation', 'school', 'uniform', and 'medical bills') to conceal the purpose of their transactions (AUSTRAC, 2019). Further, payments are made through the use of a virtual private network (VPN), encryption software, and live streaming applications to ensure the privacy and security of the customer's data (ibid).

Table 5: Common patterns of financial transactions for OSEC[11]

	Common Patterns	
Payment patterns	▪ Payments are usually small in value, generally under $500 per transaction. ▪ Offenders make repeated payments to facilitators on the same day or on successive days. ▪ Payments may be spaced out over days or weeks. ▪ Offenders and facilitators may form long-term relationships and their financial history can extend many years.	
	Facilitators	Offenders
	▪ Receive small value money transactions from multiple OSEC buyers. ▪ Make payments for domain registration or to website hosting companies. ▪ Receive funds from payment processors, including digital currencies.	▪ Purchase on webcam or live streaming platforms, including those providing adult entertainment. ▪ Purchase on dating platforms, dating websites, or websites that also offer adult entertainment. ▪ Purchase on online gaming platforms or gaming stores. ▪ Make payments or international transfers to mobile wallets. ▪ Make low value but high frequency payments on digital technology products that present a risk for child sexual exploitation.
Amounts	▪ Cost of per OSEC session is estimated to be between approximately $13 and $50 USD. ▪ Higher amounts are paid depending on the nature of the child sexual exploitation material. ▪ Amount of payment for cases involving multiple children or extreme acts of sexual violence and torture can range from $500 to $1,000.	
Frequency	▪ Multiple payments can be made to a facilitator on a single day or over a series of consecutive days. ▪ Facilitators of OSEC often receive payments from multiple perpetrators concurrently. ▪ Payment is usually made before the offense is committed.	

[11] (AUSTRAC, 2022).

	Payment methods	Payment descriptions	
Payment methods and descriptions	▪ Remittance service providers ▪ Bank transfers ▪ Digital wallets and mobile money ▪ Digital currency ▪ Prepaid debit or credit cards ▪ Global phone recharge top-ups ▪ Online payment applications	▪ Family support ▪ School fees ▪ Assistance or support ▪ Medical bills ▪ Accommodation ▪ Education ▪ Financial assistance ▪ Gift ▪ Purchase of clothing and toys	▪ Uniform ▪ Description may also include declared relationship (friend, boyfriend, girlfriend, sponsor)

AMLC found that out of the 37,844 STRs on OSEC or child pornography recorded between 2019 and June 2020, 25,889 STRs (68.41%) were international remittances (AMLC, 2020b, p. 6). This indicates that OSEC is a cross-border issue in the context of the Philippines.

The majority of senders of remittances in STRs associated with OSEC or child pornography were foreign nationals residing abroad, while receivers of these remittances reside in the Philippines (ibid).

Table 6: Top countries in demand side of OSEC based on STRs related to OSEC

No	2015 to 2018		2019 to June 2020	
	Country	# of STRs	Country	# of STRs
1	US	630	US	10,927
2	Philippines	187	Saudi Arabia	1,830
3	Australia	178	Australia	1,731
4	Canada	101	Canada	1,598
5	United Kingdom	97	United Kingdom	1,401
6	Israel	61	Singapore	629
7	Singapore	36	United Arab Emirates	556
8	France	32	Italy	553
9	Germany	29	Korea	548
10	Thailand	24	Hong Kong	454
11	Sweden	21	Japan	444
12	Switzerland	20	Germany	410
13	Kuwait	19	Malaysia	377
14	Netherlands	14	Kuwait	362
15	Iceland	13	Norway	325
16	Norway	10	Qatar	317
17	New Zealand	9	France	307
18	Indonesia	8	New Zealand	224
18	Qatar	8	Netherlands	206
18	United Arab Emirates	8	Sweden	181
19	Turkey	6		
20	Belgium	5		

Table 6 shows the top countries in the demand side of OSEC from 2015 to 2018 and from 2019 to June 2020 based on STRs. This demonstrates that the majority of OSEC buyers are mostly located in European and North American countries, as well as in the Asian and Middle Eastern regions (AMLC, 2020, p. 8).

Table 7: Top 20 countries in demand side of OSEC based on based on value of international remittances

No	2015 to 2018		2019 to June 2020	
	Country	Total value (PhP)	Country	Total value (PhP)
1	US	3,450,701.00	US	39,653,456.27
2	Australia	2,245,489.00	Australia	7,562,409.10
3	Philippines	1,317,091.00	Canada	6,299,779.21
4	Canada	993,398.00	Saudi Arabia	6,141,281.95
5	Kuwait	488,477.00	United Kingdom	4,689,196.24
6	United Kingdom	298,288.00	Norway	3,072,645.69
7	Singapore	262,647.00	United Arab Emirates	2,353,090.21
8	Indonesia	181,787.00	Korea	2,264,781.49
9	Japan	174,984.00	Singapore	2,225,845.70
10	Germany	166,975.00	Italy	1,934,938.23
11	Israel	148,455.00	Japan	1,871,010.95
12	France	142,965.00	Malaysia	1,668,964.48
13	United Arab Emirates	133,599.00	Kuwait	1,594,719.91
14	Thailand	124,861.00	Hong Kong	1,566,294.61
15	Netherlands	117,791.00	Germany	1,406,674.07
16	Switzerland	116,981.00	France	1,330,068.96
17	Brazil	86,296.00	Qatar	1,242,966.18
18	New Zealand	82,755.00	Netherlands	721,049.44
19	Qatar	77,758.00	New Zealand	717,197.16
20	Sweden	56,769.00	Solomon Islands	575,643.09

Table 7 shows the top 20 countries in the demand side of OSEC based on value (in PhP) of international remittances. Reading in conjunction with Table 6, Table 7 demonstrates that most of the top 10 countries in the demand side in terms of volume of STRs are also the top 10 countries in terms of value (in PhP) of international remittances, with the exception of Hong Kong, which was replaced by Norway (AMLC, 2020, p. 8). The US, Saudi Arabia, Australia, Canada, and the United Kingdom are the consistent top five in the demand side of OSEC in terms of both volume and value of STRs (ibid).

Based on the analysis of findings on STRs associated with OSEC, the AMLC has also identified indicators and suspicious triggers to flag payments suspected of being made for OSEC (AMLC, 2020, p. 23).

These indicators and triggers are intended to inform financial institutions in detecting and reporting financial flows associated with OSEC:

- **Multiple money transfers from different senders, who are usually male and located in Western and Middle Eastern countries, to one receiver in the Philippines without a familial relation between them.**
- **Amount of money transfers is usually under PhP 10,000, with no regular pattern because of the opportunistic nature of offending.**
- **A remitter, typically a man from a Western or Middle Eastern country, generally executes low-value (PhP10,000 or less) money transfers with multiple non-relative counterparts situated in the Philippines or other Asian Pacific countries.**
- **Payments are being made to receivers in the Philippines, with whom the remitter has no legitimate connection. It is unlikely that the remitters/offenders have work or family ties to the countries the funds are being sent to.**
- **Receivers are under investigation by law enforcement for the suspicion of being part of facilitating OSEC.**
- **Remitters are known sex offenders from another country.**
- **The age gap between remitters and receivers is more than 30 years.**
- **Payment descriptions may include, among others, 'education', 'school', 'uniform', 'medical bills', or 'gift'.**
- **Facilitators may have purchased online tools or software to facilitate online streaming and/or enhance images and videos.**
- **Money remittances are usually withdrawn immediately.**
- **Transactions are also linked to website on sex trafficking of children.**

4.3. Use of cryptocurrency

Europol reports that 'Cryptocurrencies continue to be used as part of exchanges within the growing number of for-profit schemes relating to child sexual abuse material (CSAM)' (Europol, 2021, p. 3). The use of decentralized cryptocurrencies such as Bitcoin has enabled child sex offenders to remain anonymous during the buying and selling of illicit products and services, and thus evade legal repercussions. [12]This is due to the fact that virtual currencies offer a higher level of anonymity than traditional payment systems, such as credit cards, which can be easily traced. The proactive measures taken by payment system providers such as PayPal and Western Union to prevent the use of their service for illegal activities have forced buyers and sellers to resort to more anonymous payment methods such as virtual currencies (ECPAT France, 2022, p. 8). As such, there is an apparent migration of online child sexual exploitation from more traditional payment systems to anonymizing tools and (pseudo) anonymous payment systems, including virtual currencies (ibid). This trend is likely to continue, as it provides child sex offenders with an effective way to maintain a certain level of anonymity in their transactions, providing an opportunity for them to remain unidentified.

[12] Cryptocurrency is a type of digital or virtual currency and operates independently of any central bank or government and is based on a decentralised technology called blockchain. Unlike traditional forms of money, such as coins or banknotes, cryptocurrencies exist only in digital form and are stored in digital wallets. These wallets can be accessed through computers, smartphones, or specialised hardware devices. One of the key advantages of cryptocurrencies is that they allow for secure and direct peer-to-peer transactions without the need for intermediaries like banks (Michael, 2023).

The Federal Bureau of Investigation (FBI) and the European Financial Coalition (EFC) have warned of the risks associated with virtual currencies, particularly those in the form of cryptocurrencies, being used as a payment system for those looking to purchase illicit goods, including disturbing materials related to child sexual abuse (Federal Bureau of Investigation, 2012; European Financial Coalition, 2013, p.15). The relative anonymity associated with cryptocurrencies, as well as their ability to be used to transact across borders, are considered to be the main driving factors for their increasing use in buying and selling CSEM online (ECPAT International, 2017, p. 7).

The anonymous nature of cryptocurrencies is achieved through their decentralized structure (Christian, Caitlyn, & Rhianna, 2022; Niluka, Xavier, & Matthew, 2019). Transactions are recorded openly on a distributed ledger, but rather than using names or account numbers, users are identified by alphanumeric strings of random characters, known as public keys (Yaffe-Bellany, 2022). This means that digital currency transactions cannot be traced back to a specific individual, while transaction details such as the amount, date, and time of the transaction remain publicly visible (ibid). Additionally, users can further protect their anonymity by using a combination of different public keys for each transaction (Pracmatic Coder, 2019). This makes it difficult for anyone to track the same user's activity over time, as their public key will change with each transaction. Finally, users can also take advantage of the privacy-focused cryptocurrencies such as Monero, Zcash, and Dash, which offer even greater levels of anonymity than Bitcoin (Milich, 2022).

The Internet Watch Foundation (IWF) found a rapid increase in the number of websites that accept cryptocurrency payments for the purchase of child sexual content since 2015 (Internet Watch Foundation, 2022). In 2018, the IWF identified 81 sites that allowed cryptocurrency payments, while 221 were identified in 2019 and 468 in 2020 (ibid). In 2021, IWF identified 250,000 websites containing illicit content depicting the sexual exploitation of minors. Of these, 1,014 websites enabled criminals to access or purchase videos and images of children being sexually abused or raped using virtual currencies (ibid).

Table 8: Cryptocurrency reports received by IWF (2015-2022)[13]

Year	No. of crypto reports	Crypto reports compared to all reports received per year (%)
2015	4	0.15%
2016	41	1.52%
2017	93	3.44%
2018	81	3.00%
2019	221	8.18%
2020	468	17.31%
2021	1,014	37.51%
2022	781	28.89%
Total	**2,703**	**100%**

ECPAT France (2022) observed that the use of cryptocurrencies may be limited in selling and buying live streaming of OSEC because the facilitation of OSEC generally depends on more established money service businesses and banking institutions, rather than cryptocurrency.

[13] (Internet Watch Foundation, 2022).

However, when cryptocurrency is involved in selling and buying of either live streaming of OSEC or other CSEM online, law enforcement agencies and other stakeholders may not always possess the necessary expertise and resources to investigate this crime. For example, a survey conducted by CipherTrace over a three-quarter period in 2020 revealed that only 22% of bankers and financial investigators expressed a sense of assurance in recognizing crypto-related payments (CipherTrace, 2020).

Cryptocurrency transactions can sometimes be traced and identified, despite the degree of anonymity involved (ECPAT International, 2017). This is because cryptocurrency transactions are recorded on the blockchain, a public, distributed ledger (Vos, 2022). This ledger is shared between all users on the network and contains all the transactions that have ever taken place. Every transaction that takes place is assigned a unique identifier and is associated with a specific wallet address. By analyzing the data on the blockchain, it is possible to trace the source and destination of a particular transaction and identify the associated wallets and users (Yousaf, Kappos, & Meiklejohn, 2019). Using cryptocurrency can put a user's anonymity at risk if they need to reveal their identity to acquire goods or services from a third party, such as providing their address to receive a package (ECPAT International, 2017). When a person discloses identifying details, all of the anonymous purchases made associated with the same Bitcoin address can be tracked and linked to the disclosed personal data (ibid). Further, many cryptocurrency exchanges require users to provide personal information when setting up an account, making it possible to trace and identify users who are engaging in cryptocurrency transactions. The takedown of 'Welcome to Video' in 2018 revealed the fallacy of Bitcoin and other cryptocurrency transactions providing complete anonymity (Greenberg, 2022).

By analyzing the blockchain and de-anonymizing bitcoin transactions, the US Internal Revenue Service Criminal Investigation (IRS-CI) were able to track and trace all transactions on the site, pinpointing the users who were uploading and downloading child pornography, as well as finding the location of the site administrator (US Department of Justice, 2019). Eventually, this allowed the agency to identify hundreds of perpetrators of illegal activity who believed that they could remain anonymous (ibid). The incident showed that, despite the perception of anonymity afforded by Bitcoin and other cryptocurrencies, law enforcement agencies have the capacity to trace these transactions and uncover criminal activity (Warner, 2019). The success of the IRS-CI in de-anonymizing users and identifying hundreds of online predators serves as a warning to those engaging in illegal activity online—their activities may not be as untraceable as they think (Greenberg, 2022).

Text box 2: Use of cryptocurrency to buy OSEC: Welcome to Video scandal

Welcome to Video was a dark web site that specialized in selling videos of child sexual abuse. The site was created in June 2015, and by March 2018 it had over 8 terabytes of child abuse material, featuring over 250,000 videos. The site operated using a sophisticated business model that allowed customers to purchase videos using the cryptocurrency, Bitcoin. Customers had the option of buying single videos, or subscribing to an unlimited access plan, which allowed them to download as many videos as they wanted. Welcome to Video also had a referral program, whereby users who referred new customers to the site would earn a commission on their purchases. This encouraged users to spread the word about the site and helped to increase its user base. Welcome to Video generated a total of almost $353,000 in Bitcoin from thousands of transactions in its three-year operation.

The site was taken down in March 2018, following a coordinated effort by law enforcement agencies in the US, the UK, and South Korea. The investigation team sent relatively small amounts of Bitcoin—with values estimated to be between $125 and $290 USD at the time—to the Bitcoin wallets listed in Welcome to Video's payment instructions. As the Bitcoin blockchain leaves all transactions visible and verifiable, they were able to observe the currency being transferred from these wallets to another wallet. Through an examination of a Bitcoin exchange, the investigation team identified that the second wallet was registered to the name of Jong Woo Son, who was the site's operator.[14]

While investigating Welcome to Video, the IRS-CI investigators discovered that one of Welcome to Video's clients had sent cryptocurrency to a digital wallet associated with a darknet website unfamiliar to them: 'Dark Scandals' (Berwick & Wilson, 2022). This website was run in the Darknet by a 26-year-old student named Michael Mohammad who was operating the website in the Netherlands. Dark Scandals included a number of pictures and videos showing sexual exploitation of children. Initially, Dark Scandals was accepting payments from its client through PayPal. However, PayPal blocked Dark Scandals from its payment network in 2012. Mohammad then leveraged cryptography to construct a platform that became one of the most extensive marketplaces for unlawful sexual abuse materials of children. In 2020, Mohammad was arrested as a result of an international investigation conducted by US and Dutch law enforcement agencies. It was found that Mohammad had profited to the extent of €115,000 EUR in cryptocurrency from his clients by selling them OSEC and CSAM (ibid).

[14] (Greenberg, 2022).

Text box 3: Dark Scandals[15]

Dark Scandals was a website operating in the Darknet, selling OSEC and CSAM via cryptocurrency. It was taken down in 2020 through a joint international investigation by US and Dutch law enforcement agencies. During the investigation and prosecution, it was found that the site operator, Michael Mohammad, had been charging his customers in cryptocurrency since 2013 for the purchase of child sexual exploitation materials. Customers of Dark Scandals paid up to €200 EUR ($205 USD) in cryptocurrency to download video packs made up of hundreds of clips showing child sexual exploitation.

When the IRS-CI investigators came across Dark Scandals, their undercover officers sent a payment worth in Bitcoi$25 USD n to a Dark Scandals wallet. Upon this payment, the officers received a download link via email. The context of this link included two videos depicting children being sexually abused. Then, the investigators located and accessed Mohammad's email account and found that it contained messages about payments to the site's service providers, which were in Mohammad's name. In March 2020, Mohammad was arrested in in Barendrecht, the Netherlands.

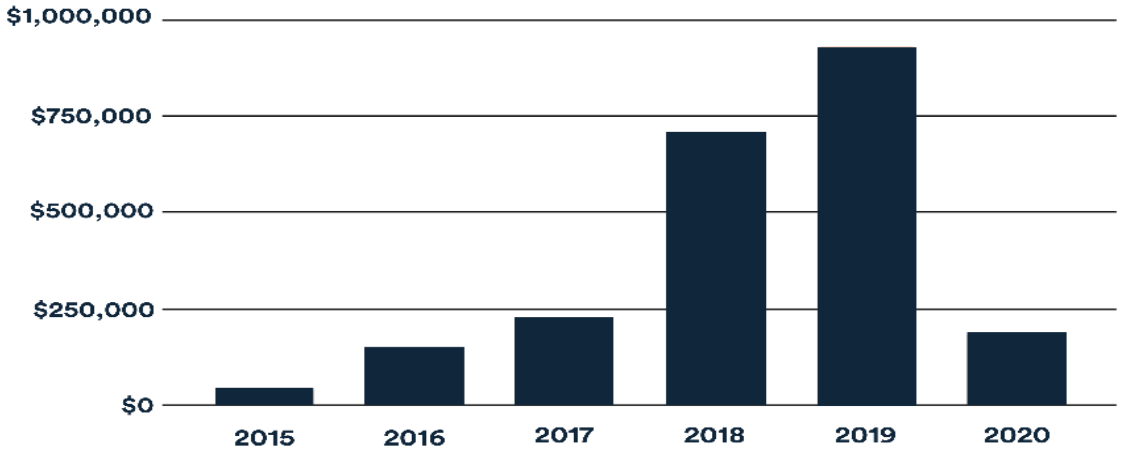
The transactions data showed that the customers of Dark Scandals used 47 different cryptocurrency exchange platforms, including Coinbase, Finland-based LocalBitcoins, and Binance. It was found that cryptocurrency worth a total of $22,000 USD moved through Coinbase and LocalBitcoins between 2013 and 2019. It was further identified that to stay anonymized, customers moved to Binance and another exchange called ShapeShift when other platforms tightened their identity checks process. During its operation, Dark Scandals received cryptocurrency worth up to €115,000 EUR. The investigation team managed to trace payments made to Dark Scandals to more than 300 accounts on eight different cryptocurrency exchange platforms. However, it was found that many customers paying to Dark Scandals used accounts opened with either no documents or false details to remain anonymous.

In 2020, Chainalysis, a company that specializes in analysing blockchain data, released a report on the utilization of digital currencies to purchase child sex abuse material on the dark web (Chainalysis, 2020). In 2019, Chainalysis monitored nearly $930,000 worth of Bitcoin and Ethereum payments to addresses connected with CSAM providers. They observed a 32% increase from 2018, which had already experienced a 212% increase from 2017.

Most of this growth was attributed to cryptocurrency usage spreading, not because of heightened demand for CSAM, although the amount involved was very small in comparison with all cryptocurrency activity (ibid).

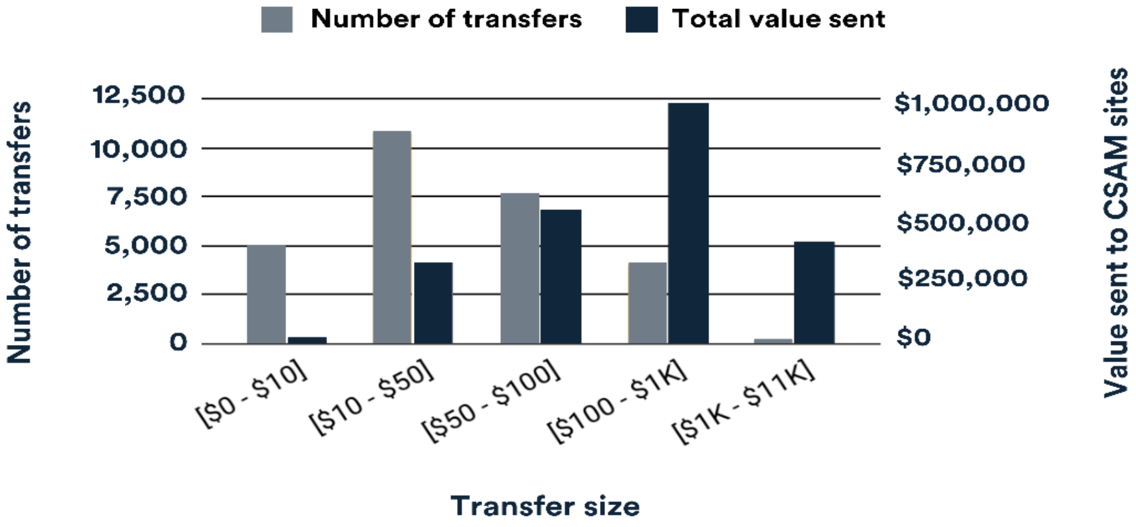
[15] (Berwick & Wilson, 2022).

Figure 5: Total value of Bitcoin in USD sent to child abuse materials site, January 2015 – March 2020[16]



Chainalysis also found that individual payments made to CSAM providers using cryptocurrencies typically fall between $10 and $50 USD, although the majority of total revenue is generated from larger payments. It was observed by law enforcement that payments within this range are indicative of either a single purchase of CSAM, or if seen on a regular basis, a subscription to a CSAM provider (ibid).

Figure 6: Number of transfers to CSAM sites and total value of Bitcoin in USD sent by transfer size, November 2013 – March 2020[17]



[16] (Chainalysis, 2020).
[17] (Chainalysis, 2020).

Several NGOs have taken initiatives to address the use of cryptocurrency to facilitate OSEC. For example, Diginex has started to develop a proof of concept for the de-anonymization of cryptocurrency transactions linked to OSEC and CSAM by examining the current state of cryptocurrency flows in the field of OSEC (Diginex, n.d.). Through the analysis of cryptocurrency flow estimates, Diginex seeks to identify and analyze the drivers and trends that inform anti-money laundering policy to provide authorities, stakeholders, and other interested parties with the knowledge, tools, and techniques necessary to effectively combat OSEC-related crime (ibid).

Similarly, IWF has launched a new ‘crypto unit’ to assist law enforcement agencies from around the world with their investigations (Internet Watch Foundation, 2022). The unit, which is receiving daily requests for information from various law enforcement organizations, has been contacted by the New Zealand police, the Austrian Criminal Intelligence Service, the Internal Revenue Service’s Criminal Investigation branch in the United States, and the Metropolitan Police in the UK. These agencies, among others, have turned to IWF's crypto unit to provide them with the information they need to investigate and prosecute OSEC crimes facilitated by cryptocurrency (ibid).

In January 2023, Tether, a company operating the blockchain-enabled platform tether.to, declared their collaboration with INHOPE, an NGO against Child Sexual Abuse Material (CSAM), to take a stand against it (Tether, 2023). Tether and INHOPE announced that Tether will be sharing data, having discussions between interested parties and taking action to eliminate the use of cryptocurrency to purchase CSAM. Tether is committed to being a leader in transparency and working with law enforcement to raise awareness of the risks associated with online CSAM marketplaces in relation to cryptocurrencies (ibid). It aims to set a standard for the industry and devise a method for cryptocurrency businesses to detect and report CSAM marketplaces more easily. Paolo Ardoino, CTO at Tether, stated that:

> Working alongside law enforcement, financial intelligence units, lawmakers and standard-setting bodies worldwide, Tether is committed to being a positive force in the crypto space by highlighting the risks of child exploitation and to help organise sensible risk mitigating controls in the cryptocurrency industry. We are especially interested in improving the ability of cryptocurrency businesses to identify transfers related to online CSAM marketplaces and report them to the authorities (ibid).

Samantha Woolfe, Head of Global Partnerships and Network Expansion at INHOPE, stated that:

> Criminals exchanging online CSA and CSE materials in financial transactions are sadly found on every technology platform today. Cryptocurrency exchange companies, hotlines and law enforcement need to seek more solutions to fight CSAM by sharing critical information and actionable intelligence with increased efficiency. To respond to this need, Tether is aware that they and other companies in the same industry must be part of this fight, especially where CSE and CSA materials are traded with cryptocurrencies. By supporting INHOPE’s work Tether is leading the way in prioritising child protection.
>
> - (INHOPE, 2023).

4.4. The role of the financial sector

It is imperative that financial institutions, law enforcement agencies, and government organizations collaborate to obstruct payments for child sexual exploitation material, thereby impeding the abuse of victims (AUSTRAC, 2022). This partnership is especially critical since financial transactions are the fundamental enablers of OSEC. Through their combined expertise and resources, these entities can identify suspicious payments and disrupt the financial networks that support the exploitation of minors. Further, partnership between these organizations can facilitate the sharing of information, enabling a more comprehensive and effective response to combat OSEC (ibid).

Financial transactions associated with OSEC can present law enforcement agencies with an invaluable opportunity to take action against those responsible (ECPAT France, 2022, p. 82). By analysing Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs), Financial Intelligence Units (FIUs) can gain insights into the networks and activities involved, as well as identify perpetrators through the information contained in them, including personally identifying information (PII) (Egmont Group of Financial Intelligence Units, 2020). Further, national FIUs are able to compile financial data from various sources, thus providing law enforcement agencies with the evidence required to launch investigations, seize and confiscate the proceeds from criminal conduct, and rescue victims (ibid). As such, this can lead to the conviction of child sex offenders, traffickers, and facilitators.

Text box 4: The importance of multi-sectoral collaboration

The issue of OSEC necessitates the involvement not only of law enforcement but also the private sector, civil society, and research organizations. The Anti-Money Laundering Council (AMLC), the Philippines' Financial Intelligence Unit (FIU), works closely with the local law enforcement, various industry partners through its Public-Private Partnership Programs (PPPP), and other jurisdictions through international coordination mechanisms, such as the Egmont Secure Web (ESW). This enables a shift from a reactive to approach to the challenge of OSEC to proactive identification of financial transactions that could be associated with OSEC. - (AMLC, 2020a, p. 5).

The Egmont Group requires all members of the private financial sector, such as banks, Money Service Businesses (MSBs), money transfer platforms, and cryptocurrency exchanges, to file SARs and STRs whenever a suspicious financial activity is identified that may be related to sex-based crimes against minors (Egmont Group of Financial Intelligence Units, 2020). The main objective of submitting these reports is to alert appropriate law enforcement agencies or organizations of potential money laundering, terrorist financing, and other criminal activity that can be identified through transactions. SARs/STRs are investigated by national Financial Intelligence Units (FIUs), and the data they contain—including PII—is used by law enforcement to identify and disrupt criminal networks (ibid). This intelligence is instrumental in identifying and prosecuting those responsible for OSEC, as well as those who traffic in, and facilitate, these offenses (ibid). The analysis of financial transactions associated with OSEC offers law enforcement the opportunity to take operational action against the perpetrators of the abuse—both those individuals viewing the content and those facilitating the abuse (ibid). FIUs may also take advantage of this data to construct an advanced profile of the criminals, enabling the development of more strategic and tactical intelligence. SARs and STRs are particularly regarded as useful tools for law enforcement as sources of intelligence, providing details about the methods used to transfer funds, as well as key identification information about the suspects (ibid).

Financial investigations can produce powerful and reliable evidence that may be used in courts of law to convict those responsible for criminal activity (ECPAT France, 2022). This underscores the importance of the financial sector having the ability to identify indicators of OSEC and establish monitoring protocols to reduce the threat of this crime. These indicators can be employed to identify potential threats, impede the individuals and organisations involved in such illegal activities, take prompt preventative measures to safeguard children from any further harm, and report such acts to law enforcement (ibid).

In September 2021, the Financial Crimes Enforcement Network (FinCEN) of the US Treasury issued an announcement to advise banking institutions to be vigilant with respect to online offenses concerning child sexual exploitation (FinCEN, 2021). The FinCEN notice gives banks detailed instructions on how to file a suspicious activity report (SAR) when dealing with potential OSEC crimes (ibid). Banks are urged to include as much information as possible in the relevant SAR field and to use specific words to indicate the type of suspicious activity. Although this call to action is meant for financial institutions in the US, it can be used globally to address OSEC by the financial sector (RedCompass, 2021).

Text box 5: Trends in OSEC crimes

FinCEN performed a review of OSEC-related SARs and observed the following trends. Between 2017 and 2020, there was a 147 percent increase in OSEC-related SAR filings, including a 17% year-over-year increase in 2020. FinCEN also observed that OSEC offenders are increasingly using convertible virtual currency (CVC) (some of which provide anonymity), peer-to-peer mobile applications, the darknet, and anonymization and encryption services to avoid detection. CVC in particular is increasingly the payment method of choice for OSEC offenders who make payments to websites that host CSAM. Finally, FinCEN found that OSEC facilitators attempt to conceal their illicit file sharing and streaming activities by transferring funds via third-party payment processors - (FinCEN, 2021).

Bibliography

Açar, K. V. (2017). Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology, 11*(1), 98-109.

AMLC. (2020). *Child Pornography in the Philippines: Post-2019 Study Using STR Data*. Retrieved January 2023, from (*http://www.amlc.gov.ph/images/PDFs/2020%20DEC%20CHILD%20PORNOGRAPHY%20IN%20THE%20PHILIPPINES%20POST-2019%20STUDY%20USING%20STR%20DATA.pdf)*

AMLC. (2020). *Online Sexual Exploitation of Children: A Crime with a Global Impact and an Evolving Transnational Threat*. Retrieved January 2023, from http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20OSEC%20AN%20EMERGING%20RISK%20AMID%20THE%20COVID19%20PANDEMIC.pdf

AUSTRAC. (2019). *Combating the sexual exploitation of children for financial gain: Activity indicators*. Retrieved January 2023, from https://www.austrac.gov.au/sites/default/files/2019-11/Fintel%20Alliance%20_Financial%20Indicators%20Report_Combating%20the%20sexual%20exploitation%20of%20children.pdf

AUSTRAC. (2022). *Combating the Sexual Exploitation of Children for Financial Gain: Financial Crime Guide*. Retrieved January 2023, from https://www.austrac.gov.au/sites/default/files/2022-12/AUSTRAC_2022_FCG_Combating_the_sexual_exploitation_of_children_web_0.pdf

Australian Federal Police. (2020). *Predators exploiting kids online during virus second wave*. Retrieved 2023 January, from https://www.afp.gov.au/news-media/media-releases/predators-exploiting-kids-online-during-virus-second-wave

Berwick, A., & Wilson, T. (2022). *Special Report: Crypto exchanges enabled online child sex-abuse profiteer*. Retrieved January 2023, from Reuters: https://www.reuters.com/legal/government/crypto-exchanges-enabled-online-child-sex-abuse-profiteer-2022-11-23/

Bracket Foundation. (2019). *Artificial Intelligence - Combating online sexual abuse of children*. Retrieved January 2023, from https://respect.international/ai-combating-online-sexual-abuse-of-children/

Brown, A. (2016). *Safe from harm: Tackling webcam child sexual abuse in the Philippines*. Retrieved January 2023, from UNICEF: https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines

Brown, R., Napier, S., & Smith, R. G. (2020). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends and Issues in Crime and Criminal Justice*(589), 1-16.

Butler, B. (2019). *Legal breaches allowed Westpac customers to pay for child sexual abuse undetected, Austrac alleges*. Retrieved January 2023, from The Guardian: https://www.theguardian.com/australia-news/2019/nov/21/legal-breaches-allowed-westpac-customers-to-pay-for-child-sex-undetected-austrac-alleges

Butler, B. (2019). *What is Westpac accused of, and how is this related to child exploitation? – explainer*. Retrieved January 2023, from The Guardian: https://www.theguardian.com/australia-news/2019/nov/21/what-is-westpac-accused-of-and-how-is-this-related-to-child-exploitation-explainer

Chainalysis. (2020, April 21). *Making Cryptocurrency Part of the Solution to Human Trafficking*. Retrieved January 2023, from https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020/

Christian, L., Caitlyn, J., & Rhianna, H. (2022). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*.

CipherTrace. (2020). *Only 22% of Bankers and Financial Investigators Feel Confident Detecting Crypto-Related Payments*. Retrieved January 2023, from https://ciphertrace.com/only-22-percent-of-bankers-feel-confident-detecting-crypto-related-payments/

Cruz, E. M., & Sajo, T. J. (2015). Exploring the Cybersex Phenomenon in the Philippines. *The Electronic Journal of Information Systems in Developing Countries, 69*(1), 1-21.

Cubitt, T., Napier, S., & Brown, R. (2021). Predicting Prolific Live Streaming of Child Sexual Abuse. *Trends and Issues in Crime and Criminal Justice*(634), 1-21.

Davy, D. (2017). *The sexual exploitation of children in Southeast Asia.* ECPAT International. Retrieved from https://www.academia.edu/36085998/The_sexual_exploitation_of_children_in_Southeast_Asia

de Leon, S. (2013). *Cyber-sex trafficking: A 21st century scourge*. Retrieved January 2023, from CNN: https://edition.cnn.com/2013/07/17/world/asia/philippines-cybersex-trafficking/index.html

Dedase-Escoton, V., Walker, S., Schurter, D., Moreno, E., Diaz, N., & Silva, S. (2020). *A Study on Online Sexual Exploitation of Children for Aftercare Reintegration*. Retrieved January 2022, from https://osec.ijm.org/documents/19/IJM-Aftercare-Reintegration_research-2021.pdf

Desara, D. (2019). *The Phenomenon of Online Live-Streaming of Child Sexual Abuse: Challenges and Legal Responses.* University of Luxembourg (Thesis).

Diginex. (n.d.). *Global Estimates on the use of digital payments in illicit online transactions*. Retrieved January 2023, from https://www.diginex.com/projects/global-estimates-on-the-use-of-digital-payments-in-illicit-online-transactions

Draper, L. (2022). *Protecting Children in the Age of End-to-End Encryption*. Retrieved January 2022, from Joint PIJIP/TLS Research Paper Series:
https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1082&context=research

ECPAT France. (2022). *Deep Dive into the Phenomenon of Live Online Child Sexual Abuse and Exploitation: How to Better Protect Children?* Retrieved January 2022, from https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2022/06/Recherche-live-streaming_web.pdf

ECPAT International. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Retrieved January 2022, from https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

ECPAT International. (2017). *Online child sexual exploitation: An analysis of emerging and selected issues*. Retrieved January 2023, from http://ecpat.de/wp-content/uploads/2018/08/Journal_No12-ebook.pdf

ECPAT, INTERPOL and UNICEF. (2022). *Disrupting Harm in the Philippines: Evidence on Online Child Sexual Exploitation and Abuse. Global Partnership to End Violence Against Children*. Retrieved January 2022, from https://www.end-violence.org/sites/default/files/2022-04/DH_Philippines_ONLINE_FINAL.pdf

ECPAT, INTERPOL, and UNICEF. (2022). *Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse*. Retrieved January 2023, from Global Partnership to End Violence Against Children: https://www.end-violence.org/sites/default/files/2022-04/DH_Philippines_ONLINE_FINAL.pdf

Egmont Group of Financial Intelligence Units. (2020). *Combatting Online Child Sexual Abuse and Exploitation through Financial Intelligence*. Retrieved January 2023, from https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2022/06/Recherche-live-streaming_web.pdf

European Financial Coalition. (2013). *Work Package 2 – Strategic Assessment of Commercial Sexual Exploitation of Children Online*. Retrieved January 2023, from https://www.safenet.bg/images/sampledata/files/efc_strategic_assessment_-_public_version.pdf

European Financial Coalition. (2015). *Strategic assessment 2014*. Retrieved January 2023, from European Financial Coalition against Commercial Sexual Exploitation of Children Online: https://www.europol.europa.eu/cms/sites/default/files/documents/efc_strategic_assessment_2014.pdf

Europol. (2016). *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. Retrieved January 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web_2016.pdf

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. Retrieved January 2023, from https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019#downloads

Europol. (2020). *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*. Retrieved January 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

Europol. (2020). *Internet Organized Crime Threat Assessment*. Retrieved January 2022, from https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Europol. (2021). *Europol Spotlight - Cryptocurrencies:Tracing the Evolution of Criminal Finance*. Retrieved January 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Federal Bureau of Investigation. (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Retrieved January 2023, from http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Financial Conduct Authority. (n.d.). *Electronic Money Issuer*. Retrieved January 2023, from https://www.handbook.fca.org.uk/handbook/glossary/G2841.html

FinCEN. (2021, September 16). *FinCEN Calls Attention to Online Child Sexual Exploitation Crimes*. Retrieved January 2023, from https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf

Garcia, L. S., & Manikan, F. Y. (2014). *Gender Violence on the Internet: The Philippine Experience*. Retrieved January 2022, from https://www.genderit.org/sites/default/files/monograph_finalz_1.pdf

Global Knowledge Partnership on Migration and Development. (2021). *Resilience COVID-19 Crisis Through a Migration Lens: Migration and Development Brief 34*. Retrieved January 2023, from https://www.knomad.org/sites/default/files/2021-05/Migration%20and%20Development%20Brief%2034_1.pdf

Greenberg, A. (2022). *Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site*. Retrieved January 2023, from Wired: https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

Grierson, J., & Weale, S. (2020, April 3). *NCA predicts rise in online child sexual abuse during coronavirus pandemic*. Retrieved January 2022, from The Guardian: https://www.theguardian.com/society/2020/apr/03/nca-predicts-rise-in-online-child-sexual-abuse-during-coronavirus-pandemic

Hernandez, S. C., Lacsina, A. C., Ylade, M. C., Aldaba, J., Lam, H. Y., Estacio, L. R., & Lopez, A. L. (2018). Sexual Exploitation and Abuse of Children Online in the Philippines: A review of online news and Articles. *Health Policy and Systems Research, 52*(4), 305-311.

Huikuri, S. (2022). *The Darkest Side of the Darknet: How Do Online Communities of Pedophiles Contribute to the Justification of Sexual Violence Against Children?* Retrieved January 2022, from https://www.theseus.fi/bitstream/handle/10024/756178/Polamk_Katsauksia_25.pdf?sequence=1

ICAEW. (n.d.). *E-money: what you need to know*. Retrieved January 2023, from https://www.icaew.com/technical/financial-services/fs-helpsheets/emoney-and-what-you-need-to-know

IJM. (2020). *Behind the Screens: A Compilation of Case Studies and Learnings about the Online Sexual Exploitation of Children*. Retrieved January 2023, from https://osec.ijm.org/documents/11/Behind_the_Screens_Fullspread_FINAL_Nov14.2020.pdf

IJM. (2020). *Falling Short: Demand-Side Sentencing for Online Sexual Exploitation of Children: Composite Case Review, Analysis, and Recommendations for the United Kingdom*. Retrieved January 2022, from https://osec.ijm.org/documents/4/FALLING_SHORT_-_Demand-side_Sentencing_-_Case_Review_October_2020.pdf

IJM. (2020). *Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society*. Retrieved January 2022, from https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020_2021-02-05-055439.pdf

Independent Inquiry Child Sexual Abuse. (2020). *The Internet: Investigation Report*. Retrieved January 2023, from https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf

INHOPE. (2023, January 26). *Tether joins fight against CSAM in Web3*. Retrieved January 2023

Internet Watch Foundation. (2018). *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse*. Retrieved January 2022, from https://www.iwf.org.uk/media/23jj3nc2/distribution-of-captures-of-live-streamed-child-sexual-abuse-final.pdf

Internet Watch Foundation. (2020). *Millions of attempts to access child sexual abuse online during lockdown*. Retrieved January 2023, from https://www.iwf.org.uk/news-media/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown/

Internet Watch Foundation. (2021). *The Annual Report*. Retrieved February 2023, from https://annualreport2021.iwf.org.uk/

Internet Watch Foundation. (2022). *New Crypto Unit formed as experts use every tool at their disposal to stop the distribution and sale of child sexual abuse images online*. Retrieved January 2023, from https://www.iwf.org.uk/news-media/news/websites-offering-cryptocurrency-payment-for-child-sexual-abuse-images-doubling-every-year/

Internet Watch Foundation. (2022). *Websites offering cryptocurrency payment for child sexual abuse images 'doubling every year'*. Retrieved January 2023, from https://www.iwf.org.uk/news-media/news/websites-offering-cryptocurrency-payment-for-child-sexual-abuse-images-doubling-every-year/

INTERPOL. (2020). *INTERPOL report highlights impact of COVID-19 on child sexual abuse*. Retrieved January 2023, from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse

Jay, A., Evans, M., Frank, I., & Sharpling, D. (2020). *Investigation Report: The Internet*. Retrieved January 2022, from Independent Inquiry Child Sexual Abuse: https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf

Kuhlmann, D. F., & Aurén, S. (2015). *Nipa Huts with High Speed Internet: Commercial Exploitation of Children in the 21st Century*. Retrieved January 2022, from https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=5424968&fileOId=5424969

Masri, L. (2015). *Webcam child sex abuse*. Retrieved January 2023, from City University of New York, Academic Works: https://academicworks.cuny.edu/gj_etds/64/

Medora, S. (2020). *eSafety office records 340% spike in complaints as coronavirus impacts online behaviour*. Retrieved January 2023, from ABC Triple J Hack: https://www.abc.net.au/triplej/programs/hack/complaints-esafety-increase-341-percent-because-coronavirus/12174654

Michael, A. (2023). What Is Cryptocurrency?. Forbes Advisor. Retrieved July 2023, from https://www.forbes.com/uk/advisor/investing/cryptocurrency/.

Microsoft. (n.d.). PhotoDNA, Retrieved July 2023, from https://www.microsoft.com/en-us/photodna

Milich, A. (2022). *The future of Zcash, Monero, and private crypto*. Retrieved January 2023, from https://skiff.org/blog/zcash-monero-private-crypto

Napier, S., Teunissen, C., & Boxall, H. (n.d.). How do child sexual abuse live streaming offenders access victims? *Trends & Issues in Crime and Criminal Justice*(642), 1-18.

NCMEC. (2019). *2019 CyberTipline Reports by Country*. Retrieved January 2023, from https://www.missingkids.org/content/dam/missingkids/pdfs/2019%20CyberTipline%20Reports%20by%20Country.pdf

NCMEC. (2020). *2020 CyberTipline Reports by Country*. Retrieved January 2023, from https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-country.pdf

NCMEC. (2021). *2021 CyberTipline Reports by Country*. Retrieved January 2023, from https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf

NCMEC. (2022). CyberTipline 2022 Report. Retrieved July 2023, from https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

NCMEC. (2022). *Our 2021 Impact*. Retrieved January 2023, from https://www.missingkids.org/content/ncmec/en/ourwork/impact.html

Niluka, A., Xavier, B., & Matthew, M. (2019). A Survey of Anonymity of Cryptocurrencies. *ACM International Conference Proceeding Series.*

Pracmatic Coder. (2019). *Is it possible to have anonymous transactions on the public blockchain?* Retrieved January 2023, from https://www.pragmaticcoders.com/blog/anonymous-transactions-on-the-public-blockchain

Ramiro, L. S., Martinez, A. B., Tan, J. R., Mariano, K., Miranda, G. M., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect, 96*, 104080.

RedCompass. (2021, October 12). *Banks can help protect children: FinCEN advises on child sexual exploitation*. Retrieved January 2023, from https://blog.redcompasslabs.com/banks-can-help-protect-children-fincen-advises-on-child-sexual-exploitation

Simantiri, N. L. (2017). *Online child sexual abuse and exploitation Current forms and good practice for prevention and protection*. Retrieved January 2023, from ECPAT International: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf

Skidmore, M., Aitkenhead, B., & Muir, R. (2022, July). *Turning the Tide Against Online Child Sexual Abuse*. Retrieved February 2023, from The Police Foundation: https://www.police-foundation.org.uk/2017/wp-content/uploads/2022/07/turning_the_tide_FINAL-.pdf

Terre des Hommes. (2013). *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines*. Retrieved January 2022, from https://www.datocms-assets.com/22233/1630916713-sweetie-background-and-psychological-impact-of-webcam-child-sex-tourism.pdf

Tether. (2023, January 26). *Tether, INHOPE Collaborate to Combat CSAM in Web3*. Retrieved from https://tether.to/es/tether-inhope-collaborate-to-combat-csam-in-web3/

The National Archives. (n.d.). *Overview*. Retrieved February 2023, from https://webarchive.nationalarchives.gov.uk/ukgwa/20221215051343/https://www.iicsa.org.uk/key-documents/15963/view/HOM003278_001-003.pdf

The World Bank. (n.d.). *Personal remittances, received (current US$) - Philippines*. Retrieved January 2023, from https://data.worldbank.org/indicator/BX.TRF.PWKR.CD.DT?locations=PH

The World Bank. (n.d.). *Poverty headcount ratio at national poverty lines (% of population) - Philippines*. Retrieved January 2022, from https://data.worldbank.org/indicator/SI.POV.NAHC?locations=PH

UNICEF. (2016). *National Baseline Study on Violence Against Children in the Philippines: 2015 National Survey Results*. Retrieved January 2022, from https://www.unicef.org/philippines/media/496/file/National%20Baseline%20Study%20on%20Violence%20Against%20Children%20in%20the%20Philippines:%20Recommendations.pdf

United Nations Office on Drugs and Crime. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. Retrieved January 2022, from United Nations: https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

US Department of Justice. (2019). *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin*. Retrieved January 2023, from https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

Varrella, A. (2017). Live Streaming of Child Sexual Abuse: Background, Legislative Frameworks and the Experience of the Philippines. *ECPAT International Journal, 12*, 47-61.

Vos, C. (2022). *Are Bitcoin transactions anonymous and traceable?* Retrieved January 2023, from https://cointelegraph.com/explained/are-bitcoin-transactions-anonymous-and-traceable#:~:text=Through%20blockchain%20explorers%2C%20one%20can,activity%20on%20the%20Bitcoin%20blockchain.

Warner, G. (2019). *"Welcome to Video" raid leads to 337 arrests due to Bitcoin Exchanges that use strong KYC*. Retrieved January 2023, from Security Boulevard: https://securityboulevard.com/2019/10/welcome-to-video-raid-leads-to-337-arrests-due-to-bitcoin-exchanges-that-use-strong-kyc/

WeProtect Global Alliance. (2018). *Threat Assessment 2018: Working together to end the sexual exploitation of children online*. Retrieved January 2023, from https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2018-EN.pdf

Yaffe-Bellany, D. (2022). *Millions for Crypto Start-Ups, No Real Names Necessary*. Retrieved January 2023, from The New York Times: https://www.nytimes.com/2022/03/02/technology/cryptocurrency-anonymity-alarm.html#:~:text=The%20ability%20to%20operate%20anonymously,interacting%20with%20traditional%20financial%20gatekeepers.

Yousaf, H., Kappos, G., & Meiklejohn, S. (2019). *Tracing Transactions Across Cryptocurrency Ledgers*. Retrieved January 2023, from USENIX Security Symposium: https://www.usenix.org/system/files/sec19-yousaf_0.pdf

University of Nottingham
Rights Lab

GLOBAL
FUND
TO
END
MODERN
SLAVERY

Discover more about our world-class research

nottingham.ac.uk/rights-lab

rightslab@nottingham.ac.uk

@rightsbeacon

Published in September 2023. The University of Nottingham has made every effort to ensure that the information in this report was accurate when published. Please note, however, that the nature of this content means that it is subject to change, therefore consider it to be guiding rather than definitive.