University of Nottingham
Rights Lab

GLOBAL FUND TO END MODERN SLAVERY

Payment methods and investigation of financial transactions in online sexual exploitation of children cases

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.

Laura Sawyer, Rights Lab Research Assistant

Sara Ciucci, Rights Lab Research Assistant

Contents

Tables

Text boxes

Table of abbreviations

ACAMS	Association of Certified Anti-Money Laundering Specialists
AMLC	Anti-Money Laundering Council (Philippines)
AUSTRAC	Australian Transaction Reports and Analysis Centre
OSAEC	Anti-Online Sexual Abuse or Exploitation of Children
CSAEM	Child Sexual Abuse or Exploitation Materials
CSAM	Child Sexual Abuse Materials
FIUs	Financial Intelligence Units
ICMEC	International Centre for Missing & Exploited Children
IJM	International Justice Mission
IWF	Internet Watch Foundation
MSBs	Money Services Businesses
NCA	National Crime Agency (UK)
OSAEC	Online Sexual Abuse or Exploitation of Children
OSCE	Organisation for Security and Cooperation in Europe
OSEC	Online Sexual Exploitation of Children
PII	Personally Identifying Information
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PPPs	Public-Private Partnerships
PSPs	Payment Services Providers
SARs	Suspicious Activity Reports
STRs	Suspicious Transaction Reports

1. Introduction

Online Sexual Exploitation of Children (OSEC) is 'a complex hidden crime that is particularly challenging for the global community to measure and address' (IJM, 2020, p. 10). As advances in technology create serious challenges for investigation and prosecution efforts, it has become easier for offenders to engage in OSEC (Europol, 2018, p. 31). Offenders benefit from technology to disguise OSEC, using internet-enabled mobile devices, anonymisation and encryption tools, new payment methods, and the Darknet to continue their activities online without disruption by law enforcement (Europol, 2020, pp. 37-38). Recent reports have found OSEC continues to grow, with a dramatic increase during the Covid-19 pandemic (ibid).

Perpetrators of OSEC use different payment methods to facilitate their crimes without being detected by law enforcement. Online payment services, money transfer services, and local payment centres are the most common payment methods in relation to livestreaming of child sexual abuse (Europol, 2018, p. 35). Perpetrators from developed countries make low value transactions once or twice a week to traffickers of OSEC in Southeast Asia, particularly the Philippines (European Financial Coalition, 2015; IJM, 2020). However, the detection of payments made for OSEC is not always easy because this pattern of money transfers is also similar to charity payments and other types of funding. Data sharing difficulties associated with privacy laws pose a further challenge to investigation of OSEC.

Cryptocurrencies and other new digital payment methods are increasingly used to facilitate OSEC (ICMEC, 2021). Both suppliers and buyers of OSEC are moving towards 'a new unregulated, unbanked digital economy' (European Financial Coalition, 2015, p. 28). Cryptocurrencies are used by suppliers to pay for hosting of websites where pictures and videos of child sexual abuse are uploaded (Europol, 2018, p. 32). Although websites in Surface Web seem to offer major payment methods, they usually seek payment outside of standard payment options when payment is processed (European Financial Coalition, 2015).

In 2019, Internet Watch Foundation (IWF) identified 288 dark websites selling materials related to OSEC, 197 of which only accept payment in virtual currencies (IWF, 2019, p. 54). The same year, Chainalysis tracked almost $930,000 worth of payments made via Bitcoin and Ethereum to addresses associated with OSEC providers, representing a 32% increase over 2018 and 212% increase over 2017 (Chainalysis, 2020). In taking down Welcome to Video, a website hosting over 250,000 unique OSEC videos, the US Department of Justice reported that OSEC customers used Bitcoin to purchase these videos (Department of Justice, 2019).

The evidence reviewed in this study and findings from interviews indicate that Money Services Businesses (MSBs) such as Western Union and PayPal continue to be the primary payment methods used for OSEC in the Philippines. This is mainly because facilitators in the Philippines as the supply side of OSEC usually dictate the ways that they want to receive the payment, and MSBs are the most convenient payment method for them.

Tracking the flow of money used to buy OSEC is crucial in preventing online child abuse and investigating and prosecuting offenders (Smedley, 2016). Proof of online payments made by offenders is often the most significant evidence for initiating an investigation, as law enforcement struggles to obtain evidence concerning live streamed OSEC, which is not stored by offenders (ECPAT Norway, 2021).

Prevention of OSEC, and investigation and prosecution of offenders, require both robust legal frameworks and effective policing and prosecution with an understating and expertise of the misuse of encryption technologies, anonymity tools, or alternative payment methods by perpetrators. This report examines the financial flows involved in OSEC cases, particularly in the Philippines, and analyses the identification and investigation OSEC-related financial transactions. The report also explores the challenges associated with traditional payment methods and new digital payment platforms, as well as cryptocurrencies used by offenders to facilitate OSEC.

2. Financial motivation behind OSEC

Participants in this study made a distinction between different OSEC cases based on whether there is a financial motivation involved in the crimes. The primary motive behind pre-recorded OSEC materials in the forms of both images and videos was reported to be the sexual gratification of offenders rather than generating financial gain (Interview #19). It was highlighted that the majority of OSEC materials are produced and shared among offenders to either get other materials for free or to gain status among other offenders (Interview #11). Given the scale of OSEC materials on the Internet, a small minority of OSEC cases are financially motivated (ibid).

Despite non-financial motives being common in OSEC cases, study participants highlighted an increasing trend in financially motivated OSEC cases, especially live streamed sexual abuse of children in Southeast Asia. This new trend was described by one participant as 'very financially driven in the way it's organised and, really unlike other forms of OSEC' (Interview #19). Sarah Napier, Research Manager of OSEC Research Programme at the Australian Institute of Criminology, explained that:

> The proportion of financially motivated crimes in that area [the Philippines] is much higher because you're dealing with vulnerable populations who, you know struggle to have basic necessities. So that's sort of where the financial element comes in. They really need money. There's plenty of offenders in Australia and Europe and America etcetera are willing to pay that money for sexual exploitation of children. - (Interview #11).

Recent reports published by Europol and the Australian Transaction Reports and Analysis Centre (AUSTRAC) showed 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 considers that OSEC, including live streaming, offers a financial incentive for criminals by creating a commercial element for OSEC (AMLC, 2020, p. 14). Typically, viewers of live streamed OSEC pay an amount to the facilitators or, in rare cases, the children directly.

Financially motivated OSEC cases mostly occur in communities that are suffering from extreme poverty or destitution. Recent studies have found that children are sexually abused by their parents and close relatives who are motivated to make economic gain (ECPAT France, 2022, p. 20). Although the monetary rewards from OSEC cases are relatively small, they are much larger than a day or week's 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.).

Participants in this study highlighted that the increasing occurrence of live streamed OSEC in the Philippines cannot only be explained by poverty. Poverty is not the main driver for this sort of crime because the majority of economically struggling families do not resort to OSEC as a source of income (Interview #18). Noel Roa Eballe, Director of National Investigations and Law Enforcement Development at International Justice Mission in the Philippines stated that:

> The reason why I made the distinction is because, personally, for me and IJM as well, we don't believe that poverty is the main driver of why OSEC happens. You can just look at other similarly economically situated families or parents who don't do this. We have cases where we have arrested perpetrators who are not really poor. So, they're not really poor and they still do this. So, I wouldn't directly conclude that it's poverty that's causing this. For me, really, I would say that yes, financial motivation, the financial aspect of it is a motivator, but I would link it not to poverty, but I would link the financial motivation of the perpetrators here to the opportunity to do it because it's a crime of opportunity ... I sincerely believe that this is a crime of opportunity. And, yes, they're motivated by money, but they are more motivated because of there is an opportunity to do it and not because they're really poor. - (Interview #18).

3. Financial transactions involved in OSEC cases

Text box 1: Typical characteristics of financial transactions in OSEC cases

- Payments from developed countries to high-risk jurisdictions
- Payments initiated by males
- Payments of low value
- Payments at irregular intervals

The most common pattern in OSEC-related transactions is low value money transfers from developed countries to high-risk jurisdictions such as the Philippines. A private sector financial representative participant in this study highlighted that individuals involved in OSEC cases usually send low dollar transfers to the Philippines using different payment platforms (Interview #1). Other research also reports similar trends in OSEC-related transactions. For example, Varrella found that the amount charged for live streamed sexual abuse shows typically ranges between ₱500 and ₱2,000 PHP, equivalent to $9 to $36 USD (Varrella, 2017, p. 49). Similarly, the European Financial Coalition also 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).

Low value transactions for OSEC poses significant challenges to identify and investigate, because this type of payment is also common in humanitarian work, religious and charity work, and online sale and commerce (Interview #1).

The pattern of OSEC-related payments resembles legitimate remittance payments which are very common between western markets and the Philippines. However, financial transactions for OSEC payments occur at irregular intervals compared to money remittances sent by Filipino migrant workers who are regularly sending money to the Philippines at regular intervals (Interview #19). Migrant workers usually send money to their families when they receive their pay checks on a weekly or monthly basis. Further, OSEC-related financial transactions are usually made in the evenings and during non-working hours (ibid).

Study participants emphasised that a significant portion of low-value transfers are primarily initiated by males from Western countries (Interview #8). Additionally, the employment status, occupation, salary, or income of individuals involved in paying for OSEC vary on a case-by-case basis. As a result, it is not possible to definitively attribute these activities to a specific population group (Interview #1).

4. Payment methods used for OSEC

Evidence reviewed in this study indicates that facilitators usually dictate which payment methods should be used by OSEC buyers to transfer money for OSEC (Interview #5). Sarah Napier, Research Manager of the OSEC Research Programme at the Australian Institute of Criminology, stated that 'it's sort of like any kind of business model where they're the ones supplying the product, and so they tell the customer how they want to be paid' (Interview #11). Facilitators usually initiate the way that money should be transferred (ibid). Neil Giles, Stop the Traffik Group Director of Intelligence and the President of Traffik Analysis Hub, explained:

> The person who holds the cards at the end of the day is the perpetrator, the delivery side of the equation. The abuser is the person who says, I need that money in this form in this place. So, the challenge for the buyer is to either negotiate that differently, or conform. Similarly, that gives challenges to the purchaser, but the purchaser has a desire to access the material, so they will take a risk if they have to. - (Interview #7).

There is a process of communication between OSEC buyers and facilitators in terms of the amount of payment and payment methods. During these communications, both parties usually reveal identifying information such as their name and payment ID (Interview #11). Such identifying information may help law enforcement to initiate investigation against parties involved in these transactions.

4.1. Credit cards and bank transfers

Participants highlighted that credit cards payments for OSEC have become 'the former way' of paying for OSEC (Interview #1). It is noted that in the early 2000s, OSEC buyers used to pay via their credit cards to access child sexual abuse materials (CSAM) on a subscription basis (Interview #15). For example, they used to buy 'club membership' for a certain amount of time (i.e., 10 hours), paying from their credit cards (ibid). However, this appears to have changed in recent years. Because of increased awareness among credit card providers such as Visa and MasterCard, use of credit cards for CSAM or OSEC has decreased (Interview #1). Although credit cards are still used for OSEC, the use of credit cards is less common. For example, out of the 50 prosecuted cases reviewed in this study, only one case included an OSEC buyer using his credit card for live streamed sexual abuse of children in the Philippines (AT5, 2013).

There has been a migration from traditional bank transfers to other payment methods such as email payments, cryptocurrency payments, and money transfer services (Interview #1). However, evidence reviewed in this research indicates that the use of bank transfers as a method of payment for the purchase of OSEC remains a serious concern. For example, the 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).1 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, 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.

[1] 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/).

4.2. Email payments

Most Payment Services Providers (PSPs) offer the ability for individuals to send payments leveraging email addresses. The buyer only needs to register their email address with their PSPs to make financial transactions simply using their email (GoCardless, 2023). After receiving the email, the recipient can request money to be deposited into any virtual banking account (Interview #1).

Email payments provide individuals with the opportunity to stay anonymous in their financial transactions (Long, 2022). A private sector financial representative participant in this study highlighted that email payments are used in grey markets and black markets engaging with selling cannabis, online gaming, and OSEC materials (Interview #1). They further emphasised that the use of emails is universal in the sense that anyone in every jurisdiction, including the Philippines, can access emails (ibid).

The ease of email payments is coupled with the ease of creating anonymous accounts. Individuals can create anonymous email accounts for free or pay with cryptocurrencies, which provides them with extra security to conceal their identity online (TroyPoint, 2022). The use of emails for money transfer guarantees more autonomy than Visa or MasterCard networks (Interview #1). It is also less risky for the person receiving the payment, as they are not required to set up a fake shell company or business to accept the payment (ibid).

Although email payments offer offenders with a new opportunity to hide their identity when making a payment for OSEC, they can also be used by law enforcement for the investigation of OSEC cases. Emails used for OSEC payments provide 'unique pieces of information' (Interview #1) that law enforcement can use as 'intelligence tools' to link an email to online suspicious activities such as OSEC. Searching for a specific email address on Google, online chat forums, or Darknet may result in direct hints to potential OSEC cases (ibid). Email payments tend to include a memo note, a specific term, slang or jargon generally used by child exploiters, which may link them to OSEC cases for further investigation (ibid).

4.3. Money transfer services

The vast majority of OSEC buyers send money via Money Service Businesses (MSBs), with payments received by facilitators through the same platform (European Financial Coalition, 2015; ECPAT, INTERPOL and UNICEF, 2022). MSBs are businesses that transmit or convert money—this includes both banks and non-bank financial institutions.2 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 sent by individuals with no family ties to the receivers (Brown, Napier, & Smith, 2020, p. 3).

[2] 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.

Study participants highlighted that MSBs are the most frequently used payment platforms in the context of the Philippines. This is because these payment services are well-established and very common in every corner of the country. For example, Brandon Kaopuiki from International Justice Mission (IJM) highlighted that 'the Philippines, in this way, is somewhat unusual on the global stage because it has such a robust money remittance infrastructure which has been built largely around the phenomena of the overseas Filipino worker' (Interview #3).

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.

While the remittance infrastructure system continues to be useful for the financial support of Filipino families, it is also being used by criminals to transfer money for OSEC from other countries. Study participants highlighted that although the use of Bitcoin and other cryptocurrencies are currently growing as methods of payment for OSEC, the use of MSBs remains the most prominent method employed in the Philippines due to those specific environmental factors (Interview #3).

The payment platform to be used for OSEC-related financial transactions is usually dictated by the supply-side (Interviews #5, #7, and #11). This also explains why MSBs are widely used in the context of the Philippines because of their availability and ease for the recipient facilitators (Interview #7). Some money remittance services can be easily accessed by facilitators at walking distance in every community in the Philippines (Interview #3). The use of money remittances enables facilitator to get money instantly, without having to wait for a few days such as in the case of a bank transfer (Interview #11). Further, MSBs are also preferred by facilitators because they are considered the most cost-efficient methods to receive payments for OSEC, compared to the high international payment fees associated with general bank transfers (Interview #12).

The frequent use of money remittances for OSEC in the Philippines is also explained by the lack of an effective mechanism to monitor and report suspicious transactions. Until very recently, local money remittance services operating in the Philippines did not generally check ID verification to establish the relationship between the sender and receiver (Interview #17). However, in 2022, the Philippines enacted the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (UNICEF Philippines, 2022). The OSAEC and CSAEM Act requires MSBs operating in the Philippines to require a valid ID and associate that ID to the person who is trying to withdraw the money (Interview #18).

There has been a migration from traditional bank transfers payments to MSBs when making OSEC-related transactions. A private sector financial representative participant in this study noted that those involved in OSEC crimes have started looking for alternative options to banks (Interview #1). MSBs are ideal payment platforms for low value transactions and do not have the same level of transaction monitoring and regulatory oversight that major banks have (ibid). Neil Giles, Stop the Traffik Group Director of Intelligence and the President of Traffik Analysis Hub, stated that MSBs provides an environment for OSEC buyers and sellers 'to hide in plain sight' because of the high volume of transactions processed by MSBs every day (Interview #7). Another advantage of using MSBs is the ability to disguise crime-related transactions with millions of legitimate transactions (ibid). Neil Giles explained that:

> In numerical terms, it's a very small percentage of the welter of criminal transactions moving through legitimate systems, hiding in plain sight. Small numbers in a very large haystack is still the best way forward. If you look back in history, some of the investigative work that identified literally tens of thousands of individuals who purchased child abuse material or access to child abuse material, it took law enforcement agencies years to work through and deal with the criminals. With some suspects, it probably took five years after they first received information before they got round to investigating an individual simply because of the volume. There's the beauty of hiding in plain sight (Interview #7).

4.4. Cryptocurrencies

All participants in this study agreed that cryptocurrencies are not often used to facilitate live streamed OSEC in the Philippines. The primary payment method in buying and selling OSEC in the Philippines remains MSBs. However, this does not mean that cryptocurrencies are never used for these purposes. Evidence reviewed in this syudy shows that 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). 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 anonymous nature of cryptocurrencies is achieved through their decentralised structure (Leuprecht, Jenkins, & Hamilton, 2023; Amarasinghe, Boyen, & McKague, 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). 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. Users can also take advantage of privacy-focused cryptocurrencies such as Monero, Zcash, and Dash, which offer even greater levels of anonymity than Bitcoin (Milich, 2022).

Study participants highlighted that the primary driver in using cryptocurrencies for CSAM is their ability to offer encryption and anonymity (Interview #1). A private sector financial representative noted that cryptocurrencies enable offenders not to be easily traced and identified, and carry out transactions freely, without the need to ask anyone's permission (ibid). Further, given that cryptocurrencies constitute a form of new technology, law enforcement agencies struggle to develop adequate instruments to individuate offenders using these payment methods for OSEC-related transactions (Interview #4).

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). Further, IJM has received 2,703 reports between 2015 and 2022, where cryptocurrency was used as payments to access or buy images and videos of children suffering sexual abuse and exploitation (see Table 1 below).

Table 1: Cryptocurrency reports received by IWF (2015-2022)[3]

Year	No. of crypto reports
2015	4
2016	41
2017	93
2018	81
2019	221
2020	468
2021	1,014
2022	781
Total	2,703

Study participants highlighted that the use of cryptocurrency to purchase live streamed OSEC from the Philippines is currently in its infancy, being limited to a few minor cases. Noel Roa Eballe, Director of National Investigations and Law Enforcement Development at IJM in the Philippines stated that cryptocurrencies are used by a minority of offenders operating on a more organised crime network basis with the ability to understand the use of cryptocurrencies for this purpose (Interview #18). He explained that ordinary individual facilitators in the Philippines do not generally have the knowledge to accept cryptocurrency payments (ibid).

Low reliance on cryptocurrencies in the context of the Philippines is also explained by the fact that they are not yet efficient enough to deal with quick transactions compared to financial transactions processed by MSBs (Interview #7). Shauna Tomkins from AMLakas Corporation noted that OSEC crimes are also generally facilitated by people in need, who prefer to receive the payment in a way that they can actually use, such as cash (Interview #13). Therefore, cryptocurrencies do not currently constitute an effective payment method for facilitators in the Philippines.

Although the use of cryptocurrencies for the purchase of OSEC does not appear to be a preferred payment method by facilitators in the Philippines, participants in the study highlighted that there is an increasing trend to use cryptocurrencies for other forms of CSAM online (Interview #4). For example, Tarana Baghirova, Programme Officer of the Organisation for Security and Cooperation in Europe (OSCE), stated that Bitcoin have been used as a means of payment for purchasing child sexual abuse material and child pornography in North America, after the blockage of credit card payments for pornography websites (Interview #6). Similarly, Colin Radcliffe from the Child Exploitation and Online Protection team at the National Crime Agency (NCA) highlighted that cryptocurrencies are likely to become more popular and their use will increase in the purchase of CSAM online in the near future (Interview #2).

[3] (Internet Watch Foundation, 2022).

5. Value of financial transactions in OSEC investigations

Criminal investigations in OSEC cases are highly victim-reliant, depending on child victims' testimony to secure a conviction. Investigations may be dropped when there are no victims to testify (Interview #6). This gap can be filled by financial transactions, linking payments to child sexual abuse.

Financial transactions alone are not considered sufficient to convict someone for OSEC. Rather, financial transactions can support the investigation as secondary evidence by establishing the link between the demand and supply side (Interview #8). Identification of financial transactions associated with OSEC can help law enforcement and the financial sector to understand trends in this sort of criminal activities. Amy Crocker, Head of Child Protection and Technology at ECPAT International, stated:

> Financial transactions are useful in a few different ways. They're useful to help us understand trends in the problem, in terms of where the exploitation is taking place, between which countries, between which types of people, you know, who is facilitating the abuse of children, who is perpetrating, etcetera. I think more concretely, and that would be the primary goal of law enforcement and the companies I think, is to identify people, perpetrators, offenders and stop them behaving, stop them exploiting children, and thereby safeguard children, if those children will be identified. So, I think that's essential. I think it then, and that data, partly through the trend analysis, but also just in general, will allow the banks to build better systems, better blocking detection, reporting systems, because the more they know about the problem, the more they can identify it and figure out what to do. - (Interview #8).

Participants highlighted that financial transactions do not have sufficient evidential value in their own to convict an offender. This is basically because a payment may be made for any purposes. Therefore, other evidence would be needed to link the payment to an OSEC case, without which an investigation is unlikely to succeed a conviction (Interview #2 and Interview #8). Colin Radcliffe from the Child Exploitation and Online Protection team at the NCA stated that:

> [Financial transactions] can never convict anyone alone. Because again, it comes back to the question of what am I paying for and what are you providing? And that is always the sticking point with live streaming, in particular, where images are not recorded. How do we prove that the payment was, say, for abuse against children and not just adult pornography? That is one of the biggest challenges of live streaming investigations. The money gives you the intelligence, but you have to get your evidence through other means. The payment of money is just supporting evidence that you would use it. You would not convict alone on payments. (Interview #2).

Financial transactions have three key benefits for the investigation of OSEC cases:

1. Alerting relevant actors of a potential crime;
2. Helping to identify perpetrators; and
3. Helping to draw links to demand side perpetrators.

5.1. Alerting of the crime

Investigations into financial transactions associated with OSEC are important because they can provide the initial evidence or intelligence to alert relevant actors that the crime may be occurring in particular locations. Shauna Tomkins from AMLakas Corporation highlighted that law enforcement can treat financial transactions as a useful starting point in investigating OSEC cases, given other challenges associated with this kind of offending such as the use of encryption and anonymisation tools (Interview #13).

5.2. Identifying perpetrators

Financial transactions associated with OSEC help law enforcement to locate offenders involved in this crime. Law enforcement often struggle to gather evidence to initiative an investigation in OSEC cases, especially live streamed child sexual abuse. The added value of financial transactions is to allow law enforcement 'to follow the money' to identify potential offenders and build their cases (Interview #4 and Interview #10). This becomes particularly important, given the high volume of CSAM and OSEC content over the Internet. Once financial transactions point out certain potential offenders, law enforcement can prioritise the investigation of these offenders compared to some other unknown online offenders (Interview #3). Brandon Kaopuiki, an IJM representative, stated that:

> So, in my view, particularly in the Philippines law enforcement context, the financial information is most helpful first as a means of targeting suspected offenders. If, for example, we have a large volume of reports and some reports include suspicious patterns of communication, whereas someone in the Philippines is communicating with somebody in the US through text and video but we can't see any of the messages, we can't see any of the images, it may look suspicious, but there's very little to act on. If we add on to that, in addition to the text and the video communication to which we don't have access because it's not being screened by the tech companies, or maybe it's encrypted, so it's not available to be screened. If we have that, plus records of financial transactions from the American to the Filipino, that gives a little bit better picture and now suspicion would increase about what's happening there. So, we have that case versus a case without the financial transactions. I would recommend, from an investigative perspective, let's prioritize the case with the financial transactions. There appears to be more indicators of possible criminality there. - (Interview #3).

5.3. Linking to demand side perpetrators

Financial transactions associated with OSEC crimes can link the crime to the demand side of OSEC. There is a financial motivation behind live streamed OSEC in the Philippines, which involves both a buyer (demand side) and a seller (supply side). Although the sexual abuse is usually carried out by sellers (or facilitators), the abuse is in fact initiated by the buyer through payments or promise of payments. Therefore, financial transactions can help identify the demand side to hold them accountable for OSEC. Noel Roa Eballe, Director of National Investigations and Law Enforcement Development at International Justice Mission in the Philippines explained:

> When we trace the financial transactions, it leads us to taking accountability on the demand side customers because it links demand side customers. The question of who is sending money to this Filipino perpetrator is already answered and it's very important in the context of OSEC because we know that OSEC is a global crime. It doesn't involve only the Filipino perpetrator who sort of supplies the child sexual abuse materials. There is also a component of the demand side – the one who purchases or the one who buys the child sexual abuse materials [from] another part of the world. So, it's very important to trace those transactions in order to hold the perpetrators and the other side of the world, the demand side, also accountable in this crime (Interview #18).

6. Role of the financial sector

The financial sector could play a huge role in the identification and prevention of OSEC crimes. This is because the financial sector is required to detect and report any transactions relating to terrorist financing, money laundering, fraud, and other predicate crimes under national anti-money laundering laws. Tiffany Polyak, Anti-Financial Crime Associate at the Association of Certified Anti-Money Laundering Specialists (ACAMS), highlighted that the financial sector can fulfil a significant role by identifying suspicious transactions associated with OSEC, which could help law enforcement to take actions in these crimes (Interview #10).

Financial institutions, law enforcement agencies, and government should collaborate to obstruct payments for child sexual exploitation material, thereby impeding the abuse of victims (AUSTRAC, 2022). 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).

The Egmont Group requires all members of the private financial sector, such as banks, 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 organisations of potential money laundering, terrorist financing, and other criminal activity that can be identified through transactions. SARs/STRs are investigated by national 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 offences (ibid).

Domestic anti-money laundering laws impose a duty on the financial sector to monitor their system and report any suspicious transactions to the national FIUs.4 The scope of these laws may vary from one country to another. OSEC is not generally explicitly stated as a predicate crime under anti-money laundering laws. However, national FIUs take initiative to deal with OSEC-related financial transactions under anti-money laundering laws. For example, Terje Nordtveit and Kirsti Solberg Løtveit, Police Superintendents at the FIU in Norway stated that:

> …the procedure under the Anti-Money Laundering Law is a way of handling this until we have a kind of legislation. Because we cannot just close our eyes that this is not happening. We know that this is happening. We know that a lot of suspects are transferring money. The suspects are completely unknown for the police, and this is the way we and the police can identify them, by money transactions. - (Interview #14).

6.1. Monitoring financial flows in OSEC cases

Financial flows act as key opportunities to identify both perpetrators and victims who require safeguarding. The Director of Intelligence at Stop the Traffik and President of Traffik Analysis Hub, Neil Giles highlighted the importance of following patterns of transactions, as they can lead to multiple safeguarding opportunities much faster than within a traditional law enforcement investigation (Interview #7).

[4] See further Nowhere to Hide 'Legal and Institutional Responses to the Online Sexual Exploitation of Children' country case study reports on the Netherlands, Norway, the Philippines, and the United Kingdom.

Financial institutions build typologies, indicators, and red flags relating to financially motivated crimes into algorithms that can flag corresponding transactions. Due to the vast number of transactions flagged, these are reduced to the most obvious suspicious transactions, which progress to human review (Interview #15). One way that financial institutions analyse financial flow is by monitoring the behaviours and anomalies surrounding customer expenditure, as an anomaly in expenditure may alert a bank to a suspicious payment. One participant highlighted the challenge with this, explaining that flagged transactions are the result of years of monitoring, and so the monitoring system is not as effective as it could be (Interview #16).

Most participants felt that the ability of financial institutions to confidently identify and flag OSEC-related transactions is limited due to the lack of clear categorisation and regulation. It was highlighted that OSEC-related transactions may only be monitored, if any, under anti-money laundering laws. However, the logic of anti-money laundering laws is not always easily translated to monitoring OSEC-related transactions. This is because money laundering is the act of making 'dirty funds clean'. However, in the case of OSEC-related transactions, money tends to be clean in the first place, and become dirty through transmission (Interview #1). Some participants pointed out the shortcomings of anti-money laundering laws in dealing with OSEC-related transactions, highlighting that they may not constitute money laundering given that the funds are clean at the point of payment (Interview #12).

The confusion about whether OSEC-transactions can be considered money laundering is further coupled with the lack of explicit provisions making them predicate offence under anti-money laundering laws. National anti-money laundering laws do not generally specify OSEC as a predicate crime. This may have a further impact in practice in terms of whether financial institutions feel to be required to monitor these transactions.

Tarana Baghirova from OSCE identified the lack of consistent red flag indicators across banks and other financial institutions in Europe as a challenge to monitoring financial flows (Interview #6). She explained that indicators that do exist have been compiled from different continents and varying publications. Therefore, she underlined the importance of providing financial institutions with more guidance on what they should be looking for, and what to do if identified (ibid).

A private sector financial representative also highlighted the need for financial institutions to be aware of the risk that their systems and services may be used by criminals to facilitate OSEC (Interview #1). They stated that this awareness will increase their ability and knowledge to enhance the existing works in the financial sector as well as developing new mechanisms to address OSEC-related financial transactions (ibid).

Participants almost unanimously referred to the good works undertaken by Western Union and PayPal in terms of monitoring OSEC-related financial transactions. Although the systems and mechanisms used by both organisations were not detailed by any of the participants to avoid revealing their techniques, it was highlighted that the two organisations have a system in place to proactively detect suspicious behaviours and take actions against flagged users (Interview #3). Other research also reported that PayPal began as early as 2014 to 'invest resource in proactively monitoring its merchants' to avoid the usage of its services for online child sexual abuse content (Mobile Alliance Against Child Sexual Abuse Content, 2014).

Text box 2: Risk of blocked offenders shifting payment platforms

When identifying or flagging a transaction for OSEC, the financial institution can report this to national FIUs. In addition to reporting, the user's account may also be blocked from using the services. However, blocking can also present a challenge for the financial sector in preventing and tackling OSEC-related transactions because users blocked by a financial institute due to potentially illegitimate activity will move onto another service provider under the guise of the need for a legitimate account (Interview #1). Colin Radcliffe, from the Child Exploitation and Online Protection Team at the NCA explained that many offenders are not stopped by blocked accounts and will simply find another method of paying the money (Interview #2). In addition, due to privacy regulations, financial institutions are not able to alert other banks that they have blocked a user's account. This means that there is nothing in place to prevent an offender from opening a new account with another institution and continuing to initiate financial transactions for OSEC until suspended from using these services (Interview #10).

While blocking users' accounts prevents offenders from continuing to make transactions for the purchase of OSEC via that financial institution's services, participants highlighted that this may also be problematic. One participant explained that blocking an account may result in the offender finding a smaller financial institution, which may not have the same level of transaction monitoring and regulatory oversight (Interview #1). As a result, future transactions may not be identified as suspicious as quickly or as easily as by a major financial institution (ibid).

Another challenge reported by participants is the reliance on transactional evidence to investigate potential offences. If a financial institution identifies suspicious payments and immediately blocks the account, less suspects connected to the crime will be able to be identified. Colin Radcliffe, from the Child Exploitation and Online Protection Team at the NCA, suggested that financial institutions should monitor, record and report the suspicious payments, so that a better flow of intelligence can be investigated at an earlier stage, resulting in law enforcement intervening against OSEC offenders (Interview #2).

6.2. Data sharing and disclosure to law enforcement

Data sharing is an important factor in the identification, investigation, and prevention of OSEC. Amy Crocker, Head of Child Protection and Technology at ECPAT International, explained that financial institutions need to understand what to look for, the types of crime, the modus operandi, offender profile information, and how to profile their customer base (Interview #8). This data is often unavailable to be shared by law enforcement, and financial institutions are equally unable to share data freely with law enforcement due to privacy laws. Privacy and data sharing laws are linked to national context, which makes disclosure very difficult (ibid).

In the United States, sections 314A and 314B of the Patriot Act relate to information sharing provisions to provide a safe harbour for sharing information. Section 314 of the Patriot Act is an important piece of legislation, enabling law enforcement to identify, disrupt, and prevent terrorist acts and money laundering activities through cooperation among law enforcement, regulators, and financial institutions to share information (FinCEN, n.d.).

By contrast, data sharing is more strictly regulated and restricted in other countries. For example, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada restricts the ability of banks and other financial institutions to share information with financial regulators, outside of national security, terrorism, or imminent danger (Merrick & Ryan, 2019). Similarly, Thomas Andersson, from ECPAT Sweden, stated that that the Swedish bank secrecy laws hamper effective flow of data sharing between financial institutions and law enforcement. He explained that Swedish bank secrecy laws allow banks to send suspicious transaction data to the financial police, but do not

allow the financial police to transfer the same data to the Cybercrime Centre, which would be the primary law enforcement agency to act on OSEC investigations in Sweden (Interview #4).

Some participants highlighted that sharing data with law enforcement would not be an effective solution to address the financial flows involved in OSEC cases. For example, Brandon Kaopuiki from IJM noted that law enforcement or FIUs receiving reports from financial institutions tend to specialise in the crimes of fraud, money laundering, and embezzlement, rather than OSEC crimes (Interview #3). Therefore, he suggested that a mechanism should be developed to enable CyberTipline to receive financial data involved in OSEC cases (ibid).

6.3. Monitoring and investigation challenges

One challenge in monitoring OSEC-related transactions is the lack of evidence that can identify the payment made for OSEC. One participant explained that while financial transactions may be able to show the offender has made a payment to a facilitator, the offender may legitimately claim that the payment was made for legitimate purposes or an adult show. Unless the offender has made recordings or images from the live stream, law enforcement would struggle to prove that the payment was made for OSEC (Interview #19).

Colin Radcliffe, from the Child Exploitation and Online Protection team at NCA noted that the investigation should include supporting evidence to link the payment to OSEC (Interview #2). However, it is not always easy to establish the cause and intent behind financial transactions. While the financial sector can follow transactions from one person to another, it is difficult to establish the criminality on either end of the payment from the transaction alone (ibid).

6.3.1. Sexual exploitation is not prioritised

OSEC-related transactions are not always prioritised for investigation and prosecution purposes. Amy Crocker, Head of Child Protection and Technology at ECPAT International, highlighted the lack of prioritisation and specialisation within policing towards online child sexual exploitation (Interview #8). There is a high level of knowledge and skill in addressing financial crimes such as money laundering, which could be transferred and used in relation to sexual exploitation. However, there is currently a general skill gap surrounding investigating OSEC (ibid).

6.3.2. Many actors are involved in financial flows

Many actors are involved in financial flows of OSEC, resulting in the obfuscation of transaction chains (Interview #12). Within an OSEC case, the transaction may involve an offender using their bank account to transfer money to a remittance company, such as PayPal or Western Union, and then use this account to transfer money from one country to another. The remittance company may also work with domestic remittance companies, which results in the transfer of the money to a local company, where the facilitator can pick up their payment (ibid). Bindu Sharma, Policy Director at the International Centre for Missing and Exploited Children, emphasised the challenge that industry actors can only see their part of the financial flow, and are unable to see the entire transaction chain. Due to this, internal reviews may not flag a transaction as suspicious, as they see only a subset of the transaction (Interview #15).

6.3.3. Financial sector should receive feedback

The lack of feedback from law enforcement presents a challenge to financial institutions monitoring OSEC-related transactions (Interview #6).

As explained above, the financial sector monitors their systems and services under anti-money laundering laws and reports suspicious transactions to national FIUs. Participants in this study explained that the financial sector's work ends when they report to the FIUs. The need for feedback from the law enforcement and FIUs in terms of whether these reports were helpful to initiate an investigation was highlighted extensively. However, law enforcement agencies and FIUs are generally unable to communicate with the financial sectors regarding the suspicious transactions because of privacy laws. In the absence of feedback, financial institutions cannot improve on their monitoring of transactions or establish any accuracy on their detections (Interview #11).

6.3.4. Financial data is not used effectively

A final challenge to the monitoring and investigation of OSEC is the legal frameworks surrounding data protection. Bindu Sharma from ICMEC highlighted that in most countries, financial institutions are required to keep data for three months. After this point, due to the amount of ongoing interactions, financial institutions purge their stored data as they cannot store such a large amount of data in perpetuity. This is challenging when investigating OSEC crimes, as often law enforcement receives so many investigation referrals that they may not be able to respond within a three-month period. At the point that the law enforcement is able to begin investigating, a lot of the evidence has already been erased by the financial institute. As a result, investigations become significantly more challenging due to the lack of evidence (Interview #15).

7. Conclusion and Recommendations

This report shows that there is a significant role to be played by the financial sector in addressing financial transactions associated with OSEC crimes. Financial transactions are regarded as essential tools to identify both the demand and supply side of OSEC, as well as safeguarding children from exploitation. However, neither financial institutions nor law enforcement take full advantage of financial transactions data to address OSEC. Below, a range of specific recommendations are outlined for both the financial sector and law enforcement to better equip them in addressing OSEC-related financial transactions.

1. **Government, civil society, and private actors should conduct awareness raising with financial institutions on OSEC**

   Initiatives should be taken to raise the awareness of financial sector that their services and systems are used by criminals to facilitate OSEC. As highlighted by participants in this research, financial institutions do not appear to prioritise monitoring their systems for suspicious OSEC-related transactions, although they usually have an effective working system for terrorism financing, money laundering and fraud.

2. **Financial institutions, FIUs, and law enforcement should collaborate to develop and update OSEC typologies and indicators**

   Financial sector and law enforcement authorities should work together to develop robust and up-to-date guidance of typologies (indicators) for OSEC-related financial transactions. National FIUs should collaborate with financial institutions reporting to them and work towards developing common typologies and indications.

3. **Financial institutions should collaborate to establish comprehensive OSEC indicators, supported by FIUs**

   Currently, it appears that only a few financial institutions take initiatives on their own to develop typologies for their own internal monitoring purposes. This should be expanded to all financial institutions through knowledge exchange and collaboration to ensure that a comprehensive set of typologies is in place to capture OSEC-related financial transactions. National FIUs can play a significant role in taking this kind of initiative among financial institutions within the remit of their jurisdictions.

4. **National PPPs should be established or extended to cover OSEC**

   Coordinated actions should be developed through Public-Private Partnerships (PPPs). Many countries have established PPPs related to money laundering or terrorism financing. These PPPs should be extended to cover OSEC-related financial transactions, bridging the gap between financial institutions and law enforcement agencies to ensure what sort of data and information can be shared, and improve their response to OSEC.

5. **Privacy laws and policies should be reviewed to enable more effective information sharing between financial institutions and law enforcement**

   Data sharing is referred as one of the primary challenges when it comes to addressing OSEC-related financial transactions.

Both the representatives of financial sector and law enforcement agencies highlighted their inability to exchange useful information/intelligence. The primary reason behind this challenge is the strict privacy laws on handling financial data. New policy considerations are needed to overcome this challenge, ensuring that useful information/data/intelligence is passed to the appropriate authorities and relevant department of financial institutions.

6. **National laws and policies should be reviewed to allow financial institutions to report suspicious transactions to specialised law enforcement units**

Representatives of financial institutions highlighted the challenge that they are only allowed to report suspicious OSEC-related transactions to national FIUs, rather than the specialised law enforcement agency working on OSEC cases. Although FIUs are specialised units working on money laundering and terrorism financing, they may have limited resources for OSEC-related crimes. Therefore, new considerations are needed to explore the possibility of reporting OSEC-related transactions to specialised law enforcement units.

7. **National privacy laws and policies should be reviewed to allow feedback to financial institutions on OSEC cases**

Representatives of financial sector further highlighted that their duty is deemed 'completed' upon reporting to FIUs. Financial institutions are not informed what actions, if any, are taken on their reports. They underlined the importance of having feedback from FIUs in terms of the impact of their reports for investigating OSEC-crimes. This would ensure that financial institutions can improve their systems and mechanisms to better monitor OSEC-related transactions.

8. **National governments should increase resource allocation for FIUs**

Given the scale of OSEC-related transactions, FIUs do not seem to have sufficient resources to effectively handle all reports submitted to them. For example, Norway's FIU is consisted of 12 officers working on STRs associated with all kinds of predicate offences under Anti-Money Laundering Law (Interview #14). However, only two of these 12 FIU officers are specifically working on OSEC transactions. Given the high number of STRs linked to OSEC, the FIU in Norway is understaffed. Similar observations are also shared with respect to other countries' FIUs. Therefore, it should be ensured that FIUs working on OSEC-related financial transactions are sufficiently resourced.

9. **National law enforcement agencies should increase the number of officers recruited and trained to address financial aspects of OSEC**

Police units working on OSEC cases usually lack the officers specialised in financial aspect of this crime. This is reflected in the fact that law enforcement does not fully use financial evidence/intelligence in investigating OSEC and prosecuting offenders. Therefore, it should be ensured that specialised officers should be recruited and trained to address financial aspects of OSEC crimes.

10. **Financial institutions and tech companies should collaborate to respond to OSEC**

Initiatives should also be taken to ensure collaboration between financial institutions and tech companies. Given that OSEC is a crime committed via using communication technologies, tech companies and financial institutions should work together to establish 'typologies/indicators' and develop a uniform response.

Bibliography

Amarasinghe, N., Boyen, X., & McKague, M. (2019). A Survey of Anonymity of Cryptocurrencies. *ACM International Conference Proceeding Series*, 1-10.

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

AT5. (2013, March 21). *Filipijnse vrouwen zedenzaak opgepakt*. Retrieved May 2023, from https://www.at5.nl/artikelen/73167/filipijnse-vrouwen-zedenzaak-opgepakt

AUSTRAC. (2019, November). *Combating the sexual exploitation of children for financial gain: Activity indicators*. Retrieved May 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

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). *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 May 2023, from https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020/

Department of Justice. (2019, October 6). *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 May 2023, from https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

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

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 Norway. (2021, March 18). *Online Child Sexual Exploitation and Abuse: A Review of Norwegian Case Law*. Retrieved May 2023, from https://static1.squarespace.com/static/55e5a4aae4b0a8e8abf5dcac/t/6062d3248f03b063e7d4b72a/1617089319499/ECPAT+Norway+Report+Online+and+media+facilitated+child+sexual+abuse+19+March+2021.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 May 2023, from 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. (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

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

Europol. (2018). *Internet Organised Crime Threat Assessment*. Retrieved May 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2018.pdf

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. Retrieved May 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

Europol. (2020). *Internet Organised Crime Threat Assessment*. Retrieved May 2023, from https://www.europol.europa.eu/cms/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

FinCEN. (n.d.). *USA PATRIOT Act*. Retrieved May 2023, from https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

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

GoCardless. (2023, March). *What Is An Email Payment Link?* Retrieved May 2023, from https://gocardless.com/guides/posts/what-is-an-email-payment-link/

ICMEC. (2021, February). *Cryptocurrency and the Trade of Online Child Sexual Abuse Material*. Retrieved May 2023, from https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf

IJM. (2020). *Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society*. Retrieved May 2023, from https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020_2021-02-05-055439.pdf

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/

IWF. (2019). *Annual Report 2019*. Retrieved May 2023, from https://www.iwf.org.uk/about-us/who-we-are/annual-report-archive/

Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime, 30*(4), 1036-1054.

Long, H. (2022, February 23). *Ultimate Guide to Private & Anonymous Payment Methods*. Retrieved May 2023, from Restore Privacy: https://restoreprivacy.com/private-anonymous-payment-methods/

Merrick, R., & Ryan, S. (2019). Data privacy governance in the age of GDPR. *Risk Management, 66*(3), 38-43.

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

Mobile Alliance Against Child Sexual Abuse Content. (2014, March). *Preventing mobile payment services from being misused to monetise child sexual abuse content*. Retrieved May 2023, from https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2014_Report_PreventingMobilePaymentServicesFromBeingMisusedToMonetiseChildSexualAbuseContent.pdf

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

Smedley, T. (2016, January 28). *Bitcoin and darknet are making it harder to track online child abuse*. Retrieved May 2023, from The Guardian: https://www.theguardian.com/sustainable-business/2016/jan/28/bitcoin-darknet-online-child-abuse-financial-sector

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

TroyPoint. (2022, May 18). *Best Anonymous Email Providers 2023 (How To Send Anonymous Email)*. Retrieved May 2023, from https://troypoint.com/anonymous-email/

UNICEF Philippines. (2022, August 3). *SaferKidsPH statement on the enactment of Republic Act No. 11930 on the protection of children against online sexual abuse and exploitation and child sexual abuse materials*. Retrieved May 2023, from https://www.unicef.org/philippines/press-releases/saferkidsph-statement-enactment-republic-act-no-11930-protection-children-against

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

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.

Annex 1. Table of interviews

Interview No	Name of Participants	Role/Position	Institutions
Interview #1	Anonymous participant	Private sector financial representative	Anonymous
Interview #2	Colin Radcliffe	Child Exploitation and Online Protection	UK's National Crime Agency
Interview #3	Brandon Kaopuiki	Representative	International Justice Mission
Interview #4	Thomas Andersson	Representative	ECPAT Sweden
Interview #5	Anonymous Participant	Anti-trafficking researcher	Anonymous
Interview #6	Tarana Baghirova	Programme Officer	Organization for Security and Cooperation in Europe
Interview #7	Neil Giles	Stop the Traffik Group Director of Intelligence and the President of Traffik Analysis Hub	Stop the Traffik
Interview #8	Amy Crocker	Head of Child Protection and Technology	ECPAT International
Interview #9	Anonymous participant	Representative of a financial institution	Anonymous
Interview #10	Tiffany Polyak	Anti-Financial Crime Associate	Association of Certified Anti-Money Laundering Specialists
Interview #11	Sarah Napier	Research Manager of OSEC Research Programme	Australian Institute of Criminology
Interview #12	Eric Favila	-	AMLakas Corporation
Interview #13	Shauna Tomkins	-	AMLakas Corporation
Interview #14	Terje Nordtveit	Police Superintendent	Norway's FIU
Interview #14	Kirsti Solberg Løtveit	Police Superintendent	Norway's FIU
Interview #15	Bindu Sharma	Policy Director	International Centre for Missing and Exploited Children
Interview #16	Julie Crutchley	Representative	ECPAT Norway
Interview #17	Jenette Jadloc-Carredo	Representative	Center to End Online Sexual Exploitation of Children, International Justice Mission, Philippines
Interview #18	Noel Eballe	Director of National Investigations and Law Enforcement Development	International Justice Mission, Philippines
Interview #19	Anonymous participant	Anonymous	Anonymous
Interview #20	Anonymous Participant	Anti-trafficking expert	Anonymous


ONLINE
PAYMENT


B
ATM
$
CREDIT CARD
1234 0000 5678 0000

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.