REPORT

Follow the money

Payments for live streaming of child sexual abuse in the Philippines.

CHILDHOOD

WORLD CHILDHOOD FOUNDATION

FOUNDED BY H.M. QUEEN SILVIA OF SWEDEN

Publisher: World Childhood Foundation
Graphic design: Bon Relations
Printed by: Åtta45
Year: 2025
www.childhood.org

Table of contents

'Follow the money': Payments for live streaming of child sexual abuse online in the Philippines.

World Childhood Foundation

World Childhood Foundation works to prevent sexual abuse against children. With knowledge, funding and networks, we empower ideas and innovation that protect children in Sweden and internationally. We support innovative projects, contributing to long-term systemic change, while at the same time improving the lives of individual children here and now.

OUR THEMATIC AREAS

We work in the following three thematic areas: Child supportive relationships and environments, Child safety online and Child focused respons to abuse.

Child supportive relationships and environments

Child safety online

Child focused response to abuse

Within these areas, we focus on where the needs are the greatest and where our expertise and experience can make the biggest difference by:

- **Inspiring and developing new approaches,** and strengthening and disseminating proven methods to help children and families at risk.
- **Contributing to long-term systemic changes** that strengthen children's rights and protection.
- **Initiating, running and supporting strategic actions** with potential, often in partnership with grass-roots organizations.
- **Investing in innovative ideas** and helping establish new organizations.
- **Creating and strengthening networks** between initiatives, organizations, and other child rights actors.
- **Shining a light on and investing** in issues and areas that few are talking about, and even fewer are working on.

Our origin

World Childhood Foundation was founded in 1999 by HM Queen Silvia and is a religiously and politically independent, private foundation. Read more about our work at childhood.org

Stella Polaris

The Children's virtual defense force

Childhood's Stella Polaris is a four-year project that aims to coordinate, encourage, and intensify AI-related initiatives to combat child sexual abuse. By bringing together actors in Sweden with different competences, we enable closer interaction between police, prosecutors, and child rights actors on the one hand and AI experts, programmers, researchers, and technology companies on the other. By doing so, we accelerate the development and utilization of useful AI solutions in the fight against child sexual abuse. Stella Polaris is funded by the Swedish Postcode Lottery.

Glossary of terms and acronyms

TERM	DESCRIPTION
AI	Artificial intelligence
AMLC	Anti-Money Laundering Council. The AMLC is the Financial Intelligence Unit (FIU) of the Philippines.
CSAM	Child Sexual Abuse Material
Facilitator	The individual or individuals that enable child sexual abuse online. Facilitators may be involved in various activities such as recruiting victims, arranging and streaming the abuse, handling communications with online perpetrators, and managing the financial transactions associated with child sexual abuse online.
FinTech	Financial Technology. FinTech refers to the integration of technology into offerings by financial services companies to improve their use and delivery to consumers. These technologies frequently include things like Artificial Intelligence, Blockchain, and big data analytics.
FIU	Financial Intelligence Unit. FIUs are central national agencies responsible for receiving, analyzing, and disseminating intelligence related to suspicious financial activities including money laundering, terrorist financing, and other financial crimes. FIUs act as a link between financial institutions and law enforcement agencies.
ICT	Information & Communications Technology
MSB	Money Service Business. MSBs are financial entities that provide services such as currency exchange, money transfers, check cashing, and remittance services.
NGO	Non-Governmental Organization
Online perpetrator	An online perpetrator is an individual who pays to view, direct, or participate in the live streaming of child sexual abuse. These perpetrators are typically located remotely and use online platforms to connect with facilitators who arrange and broadcast the abuse. The online perpetrator financially compensates the facilitator for providing access to the exploitative content, often using digital payment methods. Recipients are on the demand-side of the child sexual abuse online transaction.
SAR	Suspicious Activity Report. A SAR is a document that financial institutions and certain other entities must file with regulatory authorities when they detect potentially suspicious activity, including money laundering, fraud, terrorist financing, human trafficking and other criminal activities.
Technology-facilitated sexual exploitation and abuse	Technology-facilitated sexual abuse and exploitation refers to the use of digital platforms and tools to groom, exploit, or harm individuals, often amplifying perpetrators' reach and minimizing their accountability.
VPN	Virtual Private Network. VPNs are services that create a secure, encrypted connections over the internet.

FACILITATORS

This report examines the issue of child sexual abuse online and references the abuses children face in this context. Though it does not provide specific case details, it outlines the general types and patterns of behavior associated with child sexual abuse online.

NOTICE OF TERMINOLOGY

The terminology selected in this report aims to describe the roles of perpetrators involved in live streaming of child sexual abuse. Despite multiple options, these were chosen to clarify which of the involved perpetrators the report is referring to. The term "online perpetrator" is used to identify the demand side individual who purchases, directs and views the live streamed abuse of children, often operating entirely within an online context.

On the supply- side, the term "facilitator" denotes the individual who receives payments for and offers to live stream the physical sexual abuse of children. The facilitator is also often times the one to carry out the physical abuse of the child. Both described parties are perpetrators engaged in illegal and harmful activities.

Foreword

Every payment tells a story.

Some speak of generosity: a child receiving their first bicycle from a faraway grandparent, or a friend sending a surprise bouquet to brighten someone's day. Others whisper of necessity: a lifeline sent to cover rent, a remittance ensuring a family's next meal, or the steady rhythm of payments that keep life's essential wheels turning. But hidden among these countless transactions, a small, sinister fraction carries the weight of unimaginable harm. These are not payments of kindness or survival—they are the currency of exploitation.

Behind them lies the orchestrated suffering of children, whose abuse is live streamed to fulfill the grotesque demands of unseen offenders. Each transaction, though fleeting, represents an unthinkable reality: the monetization of pain, the transformation of innocence into a commodity.

Despite the advances in technology, our understanding of the offenders behind these crimes remains woefully incomplete. Much of what we "know" comes from the mistakes of those who are caught—patterns shaped by the errors of a few rather than the hidden behaviors of those who evade detection.

This narrow lens limits our ability to act, leaving critical blind spots in our response. We must be more ambitious. We must not settle for assumptions drawn only from what is uncovered by chance or circumstance.

This report explores a critical hypothesis: if a recipient of funds for live streamed child sexual abuse is identified, what might we learn by following the money further? Are there other, hidden offenders yet to be identified? Patterns buried in the data? From traditional remittance systems to emerging cryptocurrencies, every transaction has the potential to reveal new insights—if we dare to look. Data is central to everything we do. Data guides our decisions, sharpens our strategies, and powers the technology we rely on to address societal challenges. Artificial intelligence, in particular, holds promise in this fight, capable of processing vast amounts of transactional data to uncover hidden networks of abuse.

But technology alone is not enough. We need clarity and courage: clarity in understanding the data we already have, and courage to use it for good. In this domain, the debate over privacy often paralyzes progress.
Yet financial transactions already exist in a realm where privacy has limits. Just as payment data is scrutinized to combat terrorism and organized crime, it should be used to protect children.

This report reminds us that the tools to fight back exist, but the will to coordinate must catch up. We need more data, better analysis, and a shared commitment to wield AI and financial intelligence for justice. The goal is not only to stop those who make mistakes, but to expose those who have perfected evasion. By refusing to settle, we can dismantle the networks that profit from this abuse and take meaningful steps toward protecting children everywhere.

Paula Guillet de Monthoux
Secretary General, World Childhood Foundation

"This report reminds us that the tools to fight back exist, but the will to coordinate must catch up."

Paula Guillet de Monthoux
Secretary General, World Childhood Foundation

Introduction

This report presents findings from exploratory research conducted by the University of Nottingham Rights Lab in collaboration with World Childhood Foundation.

The study focuses on the role of financial data in detecting, understanding, and disrupting the live streaming of child sexual abuse, a specific form of child sexual abuse online. This crime has seen a significant surge in recent years, especially during the COVID-19 pandemic, as socioeconomic challenges and increased internet access have exacerbated vulnerabilities. The Philippines, recognized as a global hotspot for such abuse, experiences a concentrated demand from online perpetrators worldwide who use digital platforms to pay for, direct, and view the abuse of children in real time.

While substantial efforts have been made to analyze and disrupt payment flows associated with child sexual abuse online, most analytical efforts prioritize the demand side, focusing on convicted perpetrators rather than the supply-side facilitators who organize and broadcast abuse. This report aims to bridge this gap by investigating how financial transaction data on identified facilitators can be used to trace additional, previously unidentified online perpetrators—typically located overseas—and uncover unknown facilitators who may perpetuate these abusive networks.

Employing both desk research and insights from interviews with stakeholders across financial, law enforcement, regulatory, and NGO sectors, the study delves into patterns, challenges, and potential interventions associated with child sexual abuse online financial transactions. Central to this investigation is the question of how financial institutions can detect and disrupt suspicious transactions linked to live streaming of child sexual abuse.

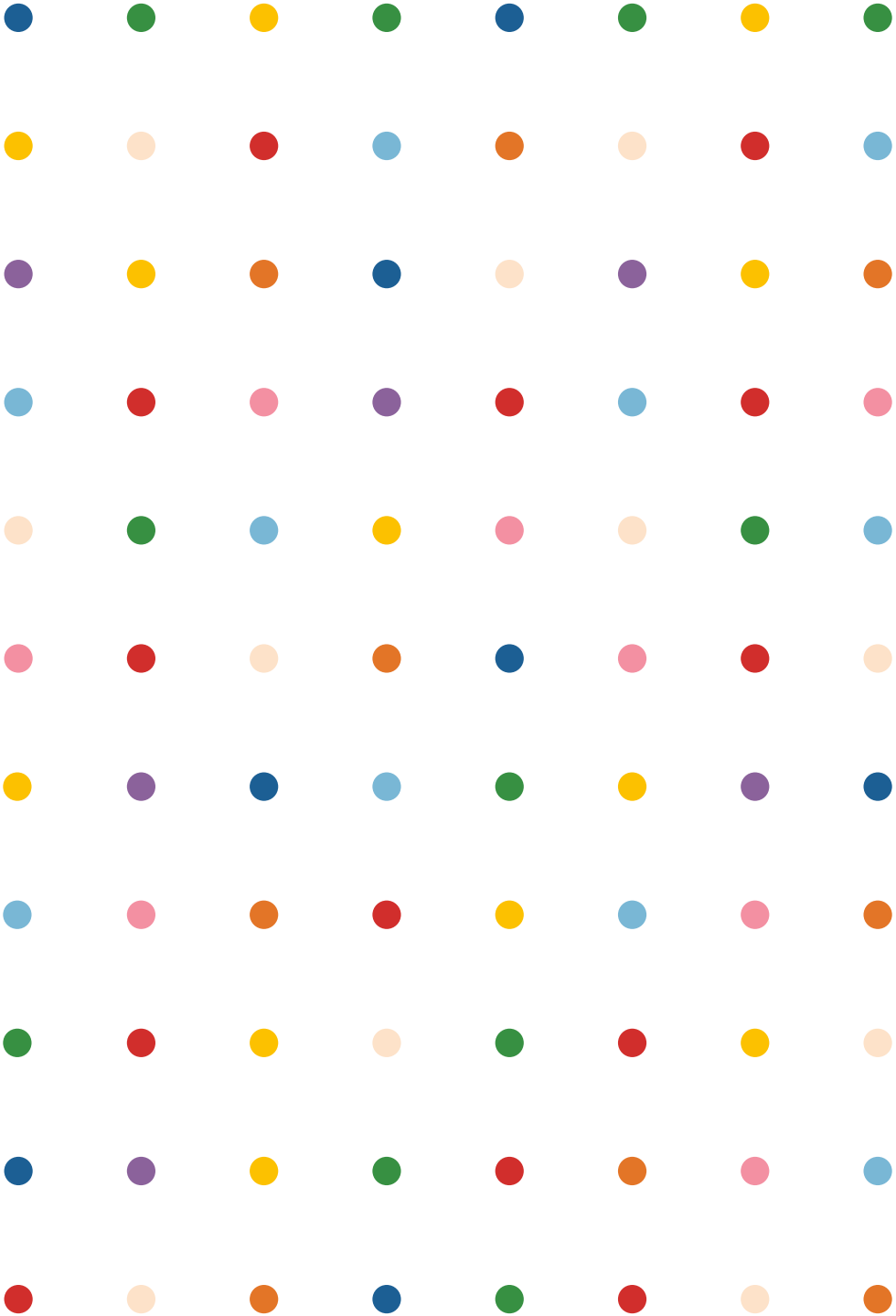
The report aims to contribute to ongoing efforts to identify and protect child victims of live streaming of child sexual abuse by exploring whether artificial intelligence (AI) could play a future role in detecting and disrupting these networks through the analysis of financial transaction data. It raises questions about how AI might assist in processing financial data and identifying patterns linked to abuse. By presenting these exploratory findings, this report aspires to stimulate further research into how AI could support interventions against this form of exploitation, by analyzing

The report aims to contribute to ongoing efforts to identify and protect child victims of live streaming of child sexual abuse.

transaction patterns, differentiating legitimate transfers from illicit ones, and supporting proactive efforts to dismantle these exploitative networks.

Ultimately, this report seeks to contribute to ongoing discussions on how collaborative actions among financial institutions, regulators, and law enforcement might improve efforts to prevent and combat the live streaming of child sexual abuse. Exploring ways to enhance information-sharing protocols, support more consistent reporting of suspicious activities, and apply advanced data analysis is critical to protecting children.

While preliminary in its findings, the report highlights that the technology and data exist to broaden the understanding of who is committing these abuses and to intercept them sooner by uncovering the traces these activities inevitably leave. Increased research and resources are essential to untangling the networks that facilitate this exploitation and to strengthen protective measures for children.



Follow the money

Payments for live streaming of child sexual abuse online in the Philippines.

Why is this important?

Child sexual abuse online refers to the use of digital platforms and technologies to sexually exploit minors.

This abuse includes the production, distribution, and consumption of child sexual abuse material (CSAM), live streamed abuse, grooming for sexual purposes, and other forms of coercive, exploitative online behavior. This includes scenarios where a perpetrator initiates contact online and then abuses the child offline. Additionally, it encompasses the production, distribution, and possession of CSAM, such as photos, videos, and live streaming.

The Philippines has been identified as the global hotspot for live streaming of child sexual abuse (IJM, 2020), with recent research by the International Justice Mission and University of Nottingham Rights Lab (2023) suggesting that the issue may have affected up to half a million children in the Philippines during 2022 alone.

The internet has had a transformative impact on child sexual abuse, reducing law enforcement's ability to disrupt perpetrators and providing platforms where perpetrators can communicate, make payments, and conduct transactions. This shift has been particularly notable in the live streaming of child sexual abuse, where online messaging, video, and payment platforms are used to facilitate the sexual exploitation of children in exchange for financial compensation (IJM, 2020).

The demand for live streaming of child sexual abuse is driven by online perpetrators who pay child sexual abuse online facilitators in the Philippines. Despite increasing international attention to the issue, empirical data on the behaviors of both perpetrators and facilitators remains limited. Existing data may be affected by underreporting, selective disclosure, the specific focus of studies, or limitations in data collection methods. Additionally, investigations and criminal convictions involving both facilitators and online perpetrators remain few, despite the scale of the problem (IJM & University of Nottingham Rights Lab, 2023). Consequently, the current understanding of child sexual abuse online in the Philippines may not fully reflect the issue's true extent.

Detecting live streaming of child sexual abuse presents distinct challenges. The transient and anonymous nature of live streams complicates identification and law enforcement efforts. Live streams typically occur in secure, encrypted

environments involving two or more parties, making it exceptionally difficult, if not impossible, to monitor such activities directly (Drejer et al., 2024).

However, the transactional aspect of live streaming of child sexual abuse provides an additional avenue to investigation and disruption efforts. The financial data is often well-documented, creating a theoretical potential to trace these transactions and uncover previously unknown online perpetrators or facilitators.

Transactions linked to live streaming of child sexual abuse may resemble or differ from other financial transactions entering the Philippines, including legitimate transfers (such as remittances from overseas workers) and illicit transactions (such as those involving exploitative adult services), which financial institutions may also flag as suspicious.

The analysis of big data, such as transaction monitoring, is well-suited for AI technologies, which are increasingly used to detect illicit activities like money laundering, terrorist financing, and the distribution of child sexual abuse material (CSAM) online.

AI offers the capability to efficiently process large volumes of complex data – such as financial transactions – identifying patterns, anomalies, and trends that indicate criminal activity.

This study examines a specific sub-category of child sexual abuse online, that of live streaming involving three distinct components (IJM, 2020):

1

The involvement of one or more facilitators who are either co-located or who live in close physical proximity to the victim(s).

2

The exchange of compensation between the online perpetrator and facilitator in return for CSAM.

3

First-generation 'newly produced' CSAM that is live streamed for the purchasing online perpetrator.

1. The online perpetrator will engage with a facilitator located in the Philippines and negotiate a price.

2. The online perpetrator transfers the agreed sum to the facilitator.

3. The facilitator live streams the child sexual abuse to the online perpetrator, often broadcasting to multiple paying perpetrators at once.

Therefore, exploring AI's potential to monitor financial transactions presents an important opportunity for understanding, identifying, and disrupting live streaming of child sexual abuse.

Using a combination of desk research and interviews with 23 key informants, this report aims to support global efforts to address child sexual abuse online across several parameters, including:

- **Understanding how transaction detection approaches** help financial institutions to detect and trace suspicious transactions that identify previously unknown online perpetrators.
- **Understanding how intelligence from financial institutions** is generated and shared to support efforts exposing the scale and nature of child sexual abuse online activities and reveal patterns of those who facilitate and drive the demand for CSAM.
- Identifying ways in which financial institutions and law enforcement can **collaborate to leverage financial transaction data to more effectively disrupt child sexual abuse online transactions** and facilitate additional investigations and arrests.
- Highlighting how improvements across these dimensions inform the **development of more effective countermeasures to detect and prevent further abuse** and ultimately aid the identification and support of child victims.

Methods

The research has been conducted in two stages.

In stage one, a rapid scoping review of literature was conducted. A search was employed on a variety of sources, including academic databases, grey literature, the websites of key national and international anti-trafficking bodies, financial institutions, international organizations, bibliographies of existing reviews of human trafficking, child sexual abuse online, and CSAM, and recommendations from key informants, colleagues and stakeholders.

A range of search terms was used to ensure relevant synonyms for, and related to, trafficking, child sexual abuse online, and CSAM were captured. The search was designed to identify all relevant literature where financial transactions linked to child sexual abuse online were especially referenced, particularly within the context of live streaming of child sexual abuse being facilitated in the Philippines. Literature was purposively screened for information relevant to our report.

Key publications from government and international bodies and Non-Governmental Organizations (NGOs) were also manually searched to identify relevant policy statements, reports, and fact sheets. Literature was analyzed for information regarding attempts to use and monitor financial transactions to detect and investigate child sexual abuse online.

In stage two, n=23 key informants were interviewed. Interviewees were purposively sampled and consisted of representatives from fintech organizations (n=2), banks and Money Service Businesses (MSBs, n=10), law enforcement (n=3), NGOs (n=2), and regulatory bodies (n=6), whose work intersects with child sexual abuse online in the Philippines. The largest representation of participants worked for organizations in the Philippines (n=12). The remainder were based in North America (n=6), Australia (n=3), and Europe (n=2). We acknowledge that the sample is potentially skewed towards participants from organizations who were keen to share practices in identifying financial transactions related to child sexual abuse online, rather than those who are not being so proactive in their efforts. Interviews were conducted in English.

Participants were asked questions regarding existing efforts to use financial transaction data to address child sexual abuse online in both proactive and responsive capacities, and regarding their engagement and collaboration with other stakeholder organizations. Interviews were recorded and transcribed before being thematically coded.

"This report explores a critical hypothesis: if a recipient of funds for live streamed child sexual abuse is identified, what might we learn by following the money further? Are there other, hidden offenders yet to be identified?"

Paula Guillet de Monthoux
Secretary General, World Childhood Foundation

Understanding live streaming of child sexual abuse

Existing data on the nature and characteristics of facilitators and online perpetrators within this context is limited and often restricted to smaller sample studies that may not capture the full scope of child sexual abuse online in the region.

Such studies include those based on interviews with convicted facilitators (Munns et al., 2024) and analyses of casework from undercover law enforcement operations (IJM, 2020).

These studies, however, provide valuable insights. According to casework by IJM, online perpetrators and facilitators in the Philippines often use established social media and online platforms to negotiate the availability and terms of live streaming of child sexual abuse. They also rely heavily on prominent payment platforms, particularly money service businesses (MSBs), to manage transactions (IJM, 2020). Facilitators prefer MSBs due to their extensive branch networks in the Philippines and the option of cash payments. The country's well-established remittance infrastructure—designed to support overseas Filipino workers sending money back to unbanked families—further facilitates this system (A. Brown, 2016; ECPAT International, 2017).

Despite political will to address the issue, gaps in resources, training, and international cooperation continue to hinder cross-border investigations and prosecutions (IJM & University of Nottingham Rights Lab, 2023).

FACILITATORS

Previous research shows that those facilitating the live streaming of child sexual abuse in the Philippines (herein 'facilitators') are primarily motivated by financial gain (AUSTRAC, 2019). Many are drawn by the prospect of 'easy money' and influenced by the contagion effects of child sexual abuse online taking place within their communities (Munns et al., 2024), along with the increased accessibility and reduced costs of technology.

With the evolving nature of technology use, there is anecdotal evidence suggesting that additional forms of child sexual abuse online are also affecting children in the Philippines. Examples include cases where children are engaged and exploited by online perpetrators directly or where additional 'brokers' exist between facilitators and online perpetrators.
For instance, recent research by Munns et al. (2024) describes facilitators' strategies, including

Attention towards child sexual abuse online in the Philippines typically refers to three facilitation scenarios:

- **Family-run operations:** These occur when one or more children are coerced to perform sexual acts by someone who is known to them (typically a parent, relative, or other caregiver).
- **Individual operations:** These are usually run from private homes or internet cafes and generally involve a single child and facilitator.
- **Larger-scale operations:** These involve a significant number of children who are hired or trafficked for child sexual abuse. Currently, there is limited evidence and documentation on this type of operation.

having older children create and share highly sexualized content on social media to attract online perpetrators. However, limited information is available to fully understand how these models intersect and/or differ from the more established types.

Lived-experience research consultants who took part in research by IJM and the University of Nottingham Rights Lab (2023), suggested that many people in the Philippines may not be aware of the specific nuances and terminology that distinguish different forms of harm, making it difficult to grasp the full extent of child sexual abuse online. This lack of distinction could obscure the dynamics unique to each scenario, including variations in the coercive actions of adults and different payment patterns. It may also reinforce a focus on the types of child sexual abuse online that have received more rigorous research and data collection.

Recent attention towards child sexual abuse online in the Philippines has largely focused on the phenomenon of individual and family-run operations facilitating online live streamed abuse. In these cases, the most commonly identified facilitators of abuse are Filipino females, including parents, family members, and other adults known to the child (UNICEF, 2021). Casework conducted by IJM (2020) on a sample of cases of child sexual

abuse online found that facilitators were often in their 20s but ranged in age from those in their teens to those who were over 70 years old. A dataset analyzed by Munns et al., (2024) identified the average age of child victims as 10 years old.

ONLINE PERPETRATORS

The demand for child sexual abuse online is sustained by online perpetrators who purchase exploitative material, contributing significantly to its prevalence. Offending of this type is most often attributed to male perpetrators from Western countries where English is widely spoken (IJM, 2020). Analysis of casework related to convicted facilitators conducted by IJM (2020) found that, while the age of online perpetrators may vary, those identified were most commonly in their 50s. However, assumptions about the demographics of online perpetrators should be treated with the same caution as that of facilitators, due to the limited data available upon which to draw conclusions.

Other research based on financial transaction data for suspected online perpetrators in Australia found that these individuals often do not have prior criminal histories (R. Brown et al., 2020). Although empirical evidence is limited, it is understood that online perpetrators may be repeat customers of individual facilitators, building rapport over time, and may purchase content from multiple facilitators simultaneously. Key informants in scoping work conducted by IJM and University of Nottingham (2023) suggested that demand-side perpetrators who purchase live streams may also possess collections of CSAM, were likely to falsify their personal details online, may escalate the severity of the content they request, and, in some cases, may travel to commit sexual offenses against children.

However, identified issues, such as perpetrator profiles, may not represent broader trends. They may instead reflect specific regional conditions, particularly in areas with greater law enforcement resources, higher rates of identified and prosecuted perpetrators, and prior research focus. Caution is therefore needed to avoid overgeneralizing these patterns. Underreporting, limited resources, and differing law enforcement priorities may mean that similar crimes go undetected or unreported in other areas.

Financial transactions related to child sexual abuse online

In this section of the report, we delve into the patterns associated with financial transactions between online perpetrators and facilitators of child sexual abuse in the Philippines, along with the economic dynamics that sustain both the supply and demand for child sexual abuse online.

It is important to note that the available evidence and data in the public domain related to these payments are limited, and there may be biases in the data due to underreporting, selective discussion, or due to the specific scope of certain studies.

PAYMENT SIZE

The size of payments for individual live streams of child sexual abuse may be subject to negotiation between the facilitator and the online perpetrator (Drejer et al., (2024). Negotiations typically occur over established encrypted online chat platforms, with prices agreed upon and payment confirmed before the live stream takes place (Napier et al., 2021). Payment amounts can depend on several factors, including the number of victims involved, their ages, and the nature and severity of the abuse (Varrella, 2017; IJM and University of Nottingham Rights Lab, 2023).

Previous reporting shows significant variation in both individual payment sizes and the cumulative amounts paid by online perpetrators to facilitators in the Philippines. For example, Munns et al. (2024) discuss payments ranging between $10 to $420 US Dollars (USD) for one-time transactions, with weekly payments around $21 USD, whereas Brown et al., (2020)

It is important to note that the available evidence and data in the public domain related to these payments are limited, and there may be biases in the data due to underreporting, selective discussion, or due to the specific scope of certain studies.

found payments with a median of approximately $50 USD, with a small number of payments exceeding $600 USD.

Analysts suggest that high-value, one-time payments may indicate increased extremity in the child sexual abuse online being purchased (AUSTRAC, 2022). However, robust evidence explaining the wide variation in individual payment sizes is limited. There is also little empirical data to confirm whether payments were made explicitly for live streaming of child sexual abuse; some payments could have been made for other reasons or as part of different arrangements between facilitators and online perpetrators.

PAYMENT PATTERNS

The significant variations in single payment size are also matched by variations in the cumulative value of payments made by individual perpetrators over time. In a dataset[1] analyzed by Munns et al. (2024), one high-volume perpetrator made payments totalling $16,953 USD over several years, whereas Brown et al., (2020) identified a suspected online perpetrator who had sent a cumulative sum exceeding $193,000 USD. In this study, a small number of buyers of child sexual abuse online were found to be responsible for a large proportion of payments made to known facilitators in the Philippines.

While nearly all suspected perpetrators whose transactions were analyzed in the second study had only made one transaction suspected of being for child sexual abuse online, conclusions from transaction data from 256 suspected online perpetrators in Australia indicated that those with histories of sexual offending were more likely to have made multiple payments for child sexual abuse online (Brown et al., 2020). Other patterns were also observed in this study, such as the average time between transactions decreasing as the volume of transactions increased, indicating that persistent online perpetrators purchased live streamed content of child sexual abuse more frequently over time.

The analysis by Brown et al., (2020) also suggests an increase in the cost of typical live streaming sessions as individuals made more transactions. Similar trends were also observed by Munns et al. (2024). While it was beyond the scope of both studies to determine what these escalating prices reflected, they speculate that perpetrators could be paying for live streaming sessions that were escalating in the severity of the sexual abuse, or that involved younger, or multiple victims (Brown et al., 2020).

As payment data in this context often relates to cases that have been detected and/or investigated during specific law enforcement operations, it is challenging to distill longitudinal trends from

this type of data. As with previous insights that have been highlighted in this report, careful consideration should be given to the potential for bias as these data come from a small sample of identified cases relative to the perceived scale of the problem. In some instances, these cases are based on analyses where suspected perpetrators were linked to a limited number of known facilitators, without subsequent validation through follow-up investigations.

TRANSACTION PROCESSES

Evidence suggests that both online perpetrators and facilitators most often use multiple well-established payment providers, including credit and debit cards, and mobile phone transactions (Munns et al., 2024). Anecdotal insights from other research suggest some evidence of a diversity of payment types being used, including email payment links, credit, debit, and crypto-currency payments (Celiksoy et al., 2023).

The most popular services used in transactions related to child sexual abuse online are said to be Money Service Businesses (MSBs), including Western Union, WorldRemit, Remitly, and PayPal (Napier et al., 2021). MSBs offer financial services such as remittances, currency exchange, and money transfers. As of June 2023, there are more than 700 different MSBs registered with the Philippines Anti Money Laundering Council (AMLC), with more than 7500 branches (BSP, 2023; AMLC, 2023). MSBs range from small, independent operations ("mom and pop shops") to larger, well-established franchises like Western Union. These services are widespread throughout the Philippines.

The remittance infrastructure in the Philippines is well-established (AMLC, 2020), and emerged to support Filipino migrants working abroad to send payments back to their families in the Philippines (A. Brown, 2016; ECPAT International, 2017). Interviews with convicted facilitators conducted by Munns et al. (2024) suggest that in some cases, facilitators may befriend employees at MSB branches so that they might turn a blind eye to suspicious payments or payment patterns (Munns et al., 2024). MSB branches are present in both urban and rural areas of the Philippines, providing easy access to cash. Cash remains the dominant currency at community level and is often favored by facilitators who may have limited or no access to formal banking channels. Cash also offers increased levels of anonymity.

There is anecdotal evidence that facilitators may systematically alternate between various MSBs to evade detection, given the requirement to present ID documentation when collecting cash. However, other evidence suggests a general absence of sophistication in concealment strategies among Filipino facilitators. For example, data from

57 investigation cases reported by IJM in 2020 indicated low use of Virtual Private Network (VPN) by facilitators in the Philippines. IJM also reported that facilitators may employ family members to collect cash, indicating the potential use of concealment tactics (IJM, 2020; IJM & University of Nottingham Rights Lab, 2023). These approaches may not be representative of facilitation trends, as the data relates to only a small number of cases that have been investigated by law enforcement in the Philippines.

On identifying potentially implicated MSBs, IJM reports that existing casework may be heavily biased towards those revealed through undercover law enforcement operations, where agents pose as online perpetrators or facilitators.[2] The MSBs identified in such operations may differ from those used by actual online perpetrators and facilitators. Identifying which MSBs are most implicated may also be skewed, as MSBs which are more proactive in flagging suspicious transactions and collaborating with international law enforcement may appear more prominently in available data.

The frequent use of money remittances for child sexual abuse online in the Philippines can also be explained by the lack of an effective mechanism to monitor and report suspicious transactions. Until recently, local money remittance services operating in the Philippines did not require ID verification to establish the relationship between the sender and receiver (Celiksoy et al., 2023). 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 request valid ID from those attempting to withdraw money (Celiksoy et al., 2023). It is unclear from the secondary evidence assessed how effective these measures have been thus far.

[1] Information on the nature of the dataset is not currently available.

[2] A small sample of undercover investigations where US law enforcement had posed as online perpetrators.

IDENTIFYING ONLINE PERPETRATORS: A CASE STUDY

A study conducted by Brown et al. (2020) demonstrates the utility of using what is known as International Funds Transfer Instruction (IFTI) reports as a promising method for identifying online perpetrators in Australia by tracking payments to people who are suspected facilitators in the Philippines. IFTIs are a regulatory requirement in Australia, and all Australian financial institutions must submit IFTIs to AUSTRAC - the Australian government's financial intelligence agency - for all international fund transfers. This includes traditional bank transfers and payment services like Western Union and other MSBs, regardless of amount.

The study used a list of 118 child sexual abuse online facilitators who had been arrested in the Philippines. These names were provided to Australian police who then passed them over to AUSTRAC. AUSTRAC was subsequently able to identify 299 Australians who had made payments to accounts linked to the arrested facilitators by analyzing IFTIs submitted to them by financial institutions in Australia. This data was then cross-referenced with other sources, such as criminal history records. Select transaction data linked to the IFTIs was provided to Brown et al. (2020) enabling additional analysis on the demographics and payment patterns of the suspected Australian online perpetrators.

This methodology has certain limitations. It is not possible from the available data to confirm whether the transactions under scrutiny were in exchange for live streams of child sexual abuse. While the names provided to AUSTRAC were persons arrested for facilitation offences of child sexual abuse online, it is possible that payments could have been made for other reasons, such as contact sexual offending (e.g., if perpetrators had physically travelled to the Philippines) or adult sexual services (not involving children). Nonetheless, the authors posited that it was unlikely that the Australian-based individuals in the study were transferring funds to recipients in the Philippines for purposes other than exploiting children. Moreover, it is important to note that the findings were derived from a small sample size and were based on a specific law enforcement investigation. The extent to which this cohort accurately represents broader financial transaction patterns indicating live streaming of child sexual abuse is unknown.

While this approach shows promise, scaling up such an approach is reliant on cooperation and information sharing between law enforcement and regulators to validate and investigate suspected online perpetrators. Further investigation into whether the online perpetrators made additional payments to accounts in the Philippines not linked to the known facilitators might provide valuable insights.

Results & discussion

Previous sections have discussed current evidence and understandings regarding the facilitation of live streaming of child sexual abuse, noting limitations of existing data. This section presents findings from interviews with key informant stakeholders (n=23).

The interviews explore the challenges and opportunities associated with using payment data to examine the income streams of facilitators and reveal previously hidden online perpetrators.

Overall, participants identified several challenges that currently inhibit the effective use of financial data to identify and investigate both facilitators and online perpetrators. Key challenges include:

- **Coordination:** Effective public-private partnerships are essential to improve information sharing and collaboration efforts, and to navigate privacy laws which are perceived as currently hindering the sharing of information between and across public and private institutions.
- **Feedback and communication:** Financial institutions perceive that there is a need for greater feedback and intelligence sharing on the use and accuracy of Suspicious Activity Reports (SARs). One participant noted feeling that SARs tended to "disappear into the abyss" once filed with regulators.
- **Resource limitations:** Both financial and regulatory institutions noted challenges related to the practical limitations of analyzing and reporting large volumes of transactions.

TRANSACTION MONITORING

Financial institutions employ transaction monitoring systems to monitor customer transactions and detect suspicious activities that might indicate a range of illegal activities, including money laundering, terrorist financing, fraud, and child sexual abuse online. These systems operate as either real-time automated systems or batch-processing systems that run at regular intervals, generating alerts for unusual transactions. Alerts may be further investigated by financial institutions themselves and compiled into Suspicious Activity Reports (SARs), which are then referred to national Financial Intelligence Units (FIUs) as part of regulatory compliance.

Interview participants revealed that approaches to monitoring transactions and submitting SARs related to child sexual abuse online vary by institution. However, there was general

consensus on the indicators and behaviors that financial institutions associate with child sexual abuse online. These indicators include multiple "low-value" payments (below $50 USD) being sent to the Philippines, where the sender does not appear to have a familial connection to the recipient (Participant #2), as well as payments for items such as VPN software, child-like sex dolls, and payments to online platforms known for hosting adult content (Participants #9, #16, #18, #21).

Participants seemed less concerned at their ability to distinguish legitimate remittance payments from suspicious payments linked to child sexual abuse online.

"When we see Filipino workers in various countries, they all have the same day off, they all get paid on the same day. So, in Singapore they get paid and the payments to the family generally come the following Sunday when they have a day off [...] those patterns around individuals become pretty obvious"

Participant #2

Overall, participants were optimistic about the strides being taken within their respective institutions to improve the accuracy of detecting transactions related to child sexual abuse online. Such approaches include the implementation of methods that rely on novel customer risk-based scoring and ranking approaches (Participant #21), developing and refining new indicator typologies (Participant #3), and conducting network analysis across their own customers to identify connections and payment patterns (Participant #8). Participant #18 described these efforts in terms of the "characteristics, behaviors, patterns and other contextual factors" that might make transactions appear inconsistent with what is expected or considered "normal" behavior.

Participant #1 further elaborated that legitimate remittance payments are consolidated so that senders can minimize transaction fees. While remittances flow regularly, payments related to child sexual abuse online can be less predictable. The opportunistic and clandestine nature of child sexual abuse online means that payments can also exhibit their own distinguishing patterns – such as taking place during evening hours in the Philippines (Munns et al., 2024).

The number of SARs related to child sexual abuse online submitted to the Philippines has increased significantly since the onset of the Covid-19 pandemic in 2020. In 2019, financial institutions and designated non-financial businesses reporting to the AMLC in the Philippines submitted 10,679 SARs related to child sexual abuse online. This figure increased to 49,532 in 2020, and further to 92,200 in 2022 (AMLC, 2023b). These increases are attributed to a rise in the prevalence of child sexual abuse online during the pandemic, rather than shifts in reporting behaviors (Participant #22). Despite this increase, there was still a perception among study participants that more explicit reporting guidelines from regulatory bodies such as the AMLC could further support efforts to improve the accuracy and consistency of suspicious activity reporting by financial institutions (#Participant 1).

Participant #8, representing an MSB, highlighted their role in the transaction process, which enables more detailed analyses of transaction networks to be conducted before SARs were filed with FIUs. This is possible because data on the "sending" side (i.e., from online perpetrators) is often extensive and may include information such as the sender's name, date of birth, email address, IP address, 16-digit card number, and other digital details. Although MSBs are often able to gather extensive data on specific transactions, access to information on senders can be limited as funds are usually transferred from other sources (Participants #3 and #8).

MSBs also generally lack insight into account-level behaviors, as money is usually transferred into the MSB from another source, such as a bank account or digital wallet. While Participant #8 expressed confidence in their capacity to identify suspect payments related to child sexual abuse online, they also expressed a degree of frustration with the lack of feedback and visibility from the AMLC and enforcement agencies in the Philippines regarding the outcomes of their reports.

They also emphasized the challenge of balancing the quantity and quality of SARs, cautioning against defensive reporting practices, which might overwhelm the system with low-assurance reports (Participant #8).

COLLABORATION AND INFORMATION SHARING

Participants generally expressed a lack of 'ground truth' data, which inhibited their ability to validate the accuracy of their detection typologies (Participant #3). There was consensus among participants that their efforts to detect payments related to child sexual abuse online from online perpetrators were significantly hampered by data constraints, primarily due to a lack of active information sharing.

Financial institutions noted insufficient feedback on how their SARs had been used and analyzed by the AMLC, as well as a lack of regular intelligence on confirmed facilitators and perpetrators (Participants #15, #8).

These gaps made it difficult for them to validate and refine their detection approaches or to train and test machine-learning-based detection models (Participant #3). Participant #8 commented:

> *"It shouldn't be this difficult [...] We know what the problem set is. We know where the hotspots of activity are. There's huge numbers of stakeholders, public sector and private sector involved in this, but it just all feels too bitty [...] It just needs better cohesion".*

Participants also discussed the challenges of distinguishing transactions related to child sexual abuse online from other payments that may exhibit similar behaviors, such as payments for adult sexual services, other forms of human trafficking, and legitimate remittance payments. Participant #15 noted that institutions and FIUs were reliant on feedback from law enforcement to provide up-to-date contextual information and insights on the use and accuracy of SARs. This sentiment was echoed by Participant #23, who indicated that they were currently unable to differentiate payments for child sexual abuse online from other types of human trafficking without feedback from law enforcement. They also suggested that the nuances of these activities were not always discernible from payment data alone.

Some participants reported efforts to corroborate payments for other goods and services, such as VPN software subscriptions, travel to the Philippines, children's clothing, child-like sex dolls, and payments to online platforms known for hosting adult content (Participants #9, #16, #18, #21). Identifying these types of payments alongside suspected transactions related to child sexual abuse online was deemed helpful, particularly in the absence of systematic and regularized intelligence sharing and feedback among FIUs, law enforcement, and reporting financial institutions (Participants #2 and #15).

The financial institutions we spoke to, which included a mix of banks and MSBs, generally agreed that while they were internally confident in their ability to detect payments related to child sexual abuse online made using their platforms, a lack of feedback from FIUs following the referral of SARs meant they had no way to validate the effectiveness and accuracy of their reporting, including identifying false positives (Participants #1, #2, #20, #21).

References to the successful use of financial transaction data to identify individuals involved in facilitating child sexual abuse

"It shouldn't be this difficult [...] We know what the problem set is. We know where the hotspots of activity are."

Participant #8

online, and online offending linked to live streaming of child sexual abuse were largely dependent on reactive efforts triggered by referrals from overseas law enforcement bodies in demand-side countries (Participants #1, #5).

These efforts were rarely initiated by agencies in the Philippines or based on proactive financial reporting. Typically, this work originated in high-volume corridors such as the UK, US, and Australia and was often conducted through ad-hoc interpersonal connections rather than established information-sharing protocols (Participant #8). In these cases, law enforcement would typically provide financial institutions with names and other payee details to cross-check against their transaction records.

Several participants noted specifically that they were unclear on what happened once their organizations submitted SARs related to child sexual abuse online to the AMLC in the Philippines. Law enforcement also indicated that they were not regularly being referred information from the AMLC regarding high-risk suspicious payments (Participants #2, #5 #9).

It was also indicated that some of the processes for reviewing, classifying, and corroborating SARs to verify reports and build intelligence from SARs were currently conducted manually by financial investigators at the AMLC, creating bottlenecks (Participant #22). Other participants called for greater capacity and financial resources to support the work of the AMLC (Participant #6), and the need for an institutional shift towards being more analytically proactive and collaborative (#Participant 2).

OPPORTUNITIES

AI-based approaches were identified as having significant potential to improve the efficiency with which transactions linked to child sexual abuse online are identified and analyzed by organizations. Some participants noted that current fraud detection methods that use machine learning approaches are already well-suited to undertake tasks such as distinguishing legitimate familial remittance from 'commercial' payments that may be indicative of child sexual abuse online or other illicit activity (Participant #1) and could be adapted for broader application.

While participants were optimistic about the potential of artificial intelligence, they were also cautious in their reflections. They pointed out that AI is not a "silver bullet solution" and stressed the importance of using high-quality data, along with careful training, testing, and validation of AI models, particularly given the limitations of the data currently available (Participants #1 and #2). However, most participants agreed that AI's ability to further automate the detection of suspicious transactions is promising.

The concept of 'link analysis' approaches was strongly advocated by financial institutions participants. Link analysis examines relationships and connections between data points to identify patterns and networks. Participants felt that this approach is not currently being taken advantage of with SARs and suggested that the AMLC could do more to identify connections between SARs submitted by different reporting financial institutions.

Analysis conducted by financial institutions themselves is typically limited to what they are able to do with their own data. To gain a more comprehensive understanding of transactions and build networks of both facilitators and online perpetrators, greater insight could be achieved through analysis conducted at a national level rather than at the institutional level. This is something the AMLC in the Philippines would be well-positioned to facilitate using SAR data.

Participant #2 elaborated:

> *"You do [the analysis] at the highest level that you possibly can to gather in all the transactions [...] then you can actually start linking those payments etc [...] particularly if they're coming from the same place, same URLs, all of this sort of stuff. So, the metadata behind the payments and who's receiving them. So is it going to the same phone number, the same address, the same names, whatever it might be".*

Participants were generally skeptical as to how much triage was currently being done by the AMLC in the Philippines, which has oversight of SARs from across payment providers, due to a lack of feedback. This concern was particularly relevant when discussing the identification and cross-referencing of known problematic names (Participant #2). Adopting such approaches could help reveal payment patterns, such as consistent transactions to specific recipients, which may not be apparent when analyzed in isolation and could differ from the typologies most commonly associated with child sexual abuse online. This strategy could be particularly useful when working backwards from known facilitators and online perpetrators. For example, if perpetrators make payments to multiple suspected facilitators, examining the metadata, such as phone numbers and addresses could help identify additional facilitators and previously unidentified online perpetrators.

Scrutinizing and delaying these transactions could also be more widely adopted as a disruptive tactic, given the immediate gratification typical in activities related to child sexual abuse online. Participants indicated that AI-based models could be used as part of the scrutinization process. For example, indicators used to identify payments related to child sexual abuse online often suggest a commercial relationship between sender and recipient (Participant #1). AI could facilitate deeper

due diligence on such payments by flagging customer profiles that behave like businesses and slowing down transactions that appear suspicious (Participant #1). Participants suggested that while such practices were already in place in some instances, they were not yet widespread based on the information gathered during interviews.

Participants emphasized that they believed the AMLC could enhance their analytical capabilities and take a more active role in combating child sexual abuse online, noting that current measures were insufficient. They argued that reports should trigger a coordinated response involving analysts, law enforcement, and other stakeholders working together to identify suspected perpetrators and facilitators. This continuous cycle of intelligence sharing emerged as a key theme among participants, underscoring the need for more proactive and consistent approaches.

This strategy could be particularly useful when working backwards from known facilitators and online perpetrators.

Conclusions

The study aimed to explore the utility of using financial data from known facilitators of child sexual abuse online to identify additional or previously unknown online perpetrators, who may also be purchasing child sexual abuse online from other currently unidentified facilitators.

Additionally, the study sought to examine limitations in current prevention and detection efforts.

The research finds that while this type of analysis is feasible, several factors hinder stakeholders—including banks, MSBs, financial regulators, and law enforcement—from effectively identifying additional online perpetrators and facilitators using financial data. Key obstacles include limited collaboration across both private and public sectors and significant data constraints linked to a lack of active data sharing. These issues affect both responsive measures, such as intercepting and disrupting payments, and proactive approaches, such as financial reporting and in-depth analysis.

Intercepting and disrupting payments between online perpetrators and facilitators based in the Philippines is crucial for enhancing the response to child sexual abuse online. This report shows the widespread implementation of payment interception approaches among multiple different actors which have substantial potential to disrupt payments linked to child sexual abuse online.

Participants reflected on several methods, currently used to varying extents, which could help identify previously unknown online

Ultimately, while this report underscores the importance of collaboration, information-sharing, and data-driven approaches, it acknowledges the complexity of this work. Moving forward, an expanded commitment to collaborative analysis and proactive data use may help create more effective safeguards for children.

perpetrators and facilitators if scaled up and adopted by more stakeholders. One such approach is for FIUs to further triangulate suspicious activity reports (SARs) across payment providers in real-time. Overall, the report indicates a consensus on the need for consistent, evidence-based monitoring and systematic feedback on SARs from FIUs to financial institutions (FIs) to improve SAR reporting and reduce false positives. One participant suggested that a shared database, accessible to FIs, regulators, and law enforcement, could achieve this goal. This highlights the need for strengthened and standardized feedback mechanisms among financial institutions, regulators, and law enforcement to validate reports and refine detection indicators and methods effectively.

Policy and practice guidelines should be formalized to improve the detection and disruption of payments related to child sexual abuse online on financial platforms. These guidelines should prioritize new, actionable solutions, enhance SAR consistency, and address training and resourcing needs for key stakeholders such as compliance officials, fraud detection specialists, anti-money laundering (AML) specialists, and law enforcement liaisons. To achieve this, effective public-private partnerships are needed to improve information sharing and collaboration, especially as financial institutions face resource constraints that impact their capacity to analyze and report large volumes of transactions.

According to participants, one of the most promising methods to identifying unknown online perpetrators lies in the implementation of linked data analysis at a national or higher level to establish a more comprehensive view of transactions and perpetrator networks. FIUs have the opportunity to leverage typologies and metadata, such as phone numbers or addresses, to identify irregular payment patterns and provide systematic intelligence to financial institutions and law enforcement, potentially revealing previously unknown online perpetrators and additional facilitators.

Ultimately, while this report underscores the importance of collaboration, information-sharing, and data-driven approaches, it acknowledges the complexity of this work. Moving forward, an expanded commitment to collaborative analysis and proactive data use may help create more effective safeguards for children. Leveraging AI and other technological solutions could eventually reduce the resource burden and enhance the detection of illicit activities—provided these tools are designed with careful consideration of the unique data requirements and ethical implications involved.

Pulling together against facilitators of live streamed child sexual abuse in the Philippines

Sandra Hernandez, Research Assistant Professor, University of the Philippines Manila

In the past 15 years, sexual abuse of children online in the Philippines has escalated along with rapidly evolving information and communication technology. The first reports in the Philippines surfaced in 2010 when police rescued minors from cybersex dens. Within ten years, law enforcement data worldwide confirmed that the Philippines had become one of the largest known sources of child sexual abuse online.

During the pandemic, the Department of Justice Office of Cybercrime reported an alarming increase in possible cases in the Philippines. By 2022, the International Justice Mission and University of Nottingham Rights Lab Scale of Harm prevalence study estimated that nearly half a million Filipino children have been trafficked to produce new child sexual abuse material.

The evidence base for child sexual abuse online in the Philippines is in its early stages. The current literature describes payment patterns using information gathered from interviews, casework, chat logs, and law enforcement data. Few studies, primarily conducted on the demand side, have analyzed payment patterns to detect and investigate the live streaming of child sexual abuse.

Financial transaction data may offer significant, although limited, insight into offender characteristics, behaviors, and modus operandi. At this time, when empirical evidence is developing, studies on financial transaction data are vital in building scientific research around child sexual abuse online in the Philippines.

Financial transaction data may also provide opportunities for detecting, disrupting, investigating, and prosecuting offenders, which requires monitoring frameworks, interagency partnerships, and collaborative solutions.

While promising, even AI-based approaches rely on data and intelligence sharing and cross-sectoral collaboration between law enforcement and the private sector. The report echoes this need for coordination, with stakeholders highlighting challenges in communication,

"In the next decade, we may turn the tide against online sexual abuse and exploitation of children."

Sandra Hernandez
Research Assistant Professor,
University of the Philippines Manila

feedback, and information-sharing between involved sectors that obstruct current efforts to use financial data.

The critical insights from the report can inform the implementation of recent leadership and legislative efforts in the Philippines. Republic Act No. 11930 or the Anti-Online Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act, which lapsed into law on July 30, 2022, explicitly criminalizes streaming and live streaming of child sexual abuse online. The Anti-OSAEC and Anti-CSAEM Act enables a more proactive and coordinated multi-stakeholder response.

The Implementing Rules and Regulations direct the flow of reports and information-sharing across sectors regarding financial data. The Anti-Money Laundering Council (AMLC) is mandated to issue guidelines to determine suspicious activity and indicators of child sexual abuse online-related activities. Payment service providers must report any suspected activity of child sexual abuse online or suspicious transactions to the Department

of Justice and the AMLC. Law enforcement may require payment service providers, financial facilitators, and other financial intermediaries to provide financial documents and information.

The law further provides for sharing information, experiences, and practices related to cases of child sexual abuse online and offline. These directives provide mechanisms for engagement between law enforcement and the financial sector, including sharing information and expertise to enhance each stakeholder's capacity.

It is important to note that on top of monitoring by the financial sector and reporting to law enforcement, the report emphasizes the essential need for two-way communication across sectors. The complex problem of child sexual abuse online requires global collaboration and a 'whole-of-society' approach, where relevant government agencies, the private sector, and civil society mutually agree and jointly pursue common solutions. On August 6, 2024, the President of the Philippines responded to the alarming and horrifying prevalence of child sexual abuse online in the Philippines by creating the Presidential Office for Child Protection. Executive Order No. 67, s. 2024 tasks the presidential Office for Child Protection with monitoring and harmonizing government policies and programs with a focus on anti-child sexual abuse online, anti-child sexual abuse material, and anti-child trafficking matters. As of 2024, the Philippines displays the highest national commitment to tackling child sexual abuse online.

The Philippine government has taken significant strides in building a comprehensive national deterrence response. The next steps lie in the urgent, strict, and complete implementation of the Anti-OSAEC and Anti-CSAEM Act and stakeholder's intensified, proactive, and coordinated efforts. While there is still much work to be done, in the next decade, we may turn the tide against online sexual abuse and exploitation of children.

"The complex problem of child sexual abuse online requires global collaboration and a 'whole-of-society' approach."

Sandra Hernandez
Research Assistant Professor,
University of the Philippines Manila

References

AMLC. (2020). Online Sexual Exploitation of Children - A crime with global impact and an evolving transnational threat. Republic of the Philippines Anti-Money Laundering Council.

AMLC. (2023). List of MSB entities registered with AMLC as of 30 June 2023. Anti Money Laundering Council.

AMLC. (2023b) Online Sexual Abuse and Exploitation of Children in the Philippines: An Evaluation using STR data. Anti Money Laundering Council.

AUSTRAC. (2019). Combating the sexual exploitation of children for financial gain - Activity indicators. Fintel Alliance.

AUSTRAC. (2022). Combating the Sexual Exploitation of Children for Financial Gain: Financial Crime Guide. Fintel Alliance.

Brown, A. (2016). Safe from harm: Tackling webcam child sexual abuse in the Philippines. UNICEF.

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. https://doi.org/10.52922/ti04336

BSP. (2023). List of BSP-Registered Money Service Business (MSBs), as of 31 March 2024. Bangko Sentral Ng Pilipinas. https://www.bsp.gov.ph/Lists/Directories/Attachments/12/MSBs.pdf

Celiksoy, E., Schwarz, K., Sawyer, L., & Ciucci, S. (2023). Payment methods and investigation of financial transactions in online sexual exploitation of children cases. University of Nottingham / Global Fund to End Modern Slavery.

Drejer, C., Riegler, M. A., Halvorsen, P., Johnson, M. S., & Baugerud, G. A. (2024). Livestreaming Technology and Online Child Sexual Exploitation and Abuse: A Scoping Review. Trauma, Violence, and Abuse, 25(1), 260–274. https://doi.org/10.1177/15248380221147564

ECPAT International. (2017). Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues. http://www.ecpat.org/wp-content/uploads/2017/04/Journal_No12-ebook.pdf

IJM. (2020). Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society. https://www.ijmuk.org

IJM, & University of Nottingham Rights Lab. (2023). Scale of Harm Research Method, Findings, and Recommendations: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines. International Justice Mission. https://www.ijm.org/studies/scale-of-harm-estimating-the-prevalence-of-trafficking-to-produce-child-sexual-exploitation-material-in-the-philippines

Munns, N., Brennan, M., Byrnes, E., Jabar, M., Tarroja, M. C., Collado, Z., & Perkins, D. (2024). Facilitation of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines. Justice & Care. https://justiceandcare.org/policies-and-reports/facilitation-of-online-sexual-abuse-and-exploitation-of-children-osaec-in-the-philippines/

Napier, S., Teunissen, C., & Boxall, H. (2021). Live streaming of child sexual abuse: an analysis of perpetrator chat logs. Live Streaming of Child Sexual Abuse: An Analysis of Perpetrator Chat Logs. https://doi.org/10.52922/ti78375

UNICEF. (2021). National Study on Online Sexual Abuse and Exploitation of Children in the Philippines. https://www.unicef.org/philippines/media/2601/file/National Study on Online Sexual Abuse and Exploitation of Children in the Philippines - Executive Summary.pdf

Varrella, A. (2017). Live streaming of sexual abuse: background, legislative frameworks and the experience of the Philippines. ECPAT International. 12.

Participants by type

PARTICIPANT NO.	ORGANIZATION TYPE	LOCATION
# 1	FinTech	Overseas
# 2	FinTech	Overseas
# 3	Bank / Money Service Business	Philippines
# 4	Bank / Money Service Business	Philippines
# 5	Law Enforcement	Philippines
# 6	Non-Governmental Organization	Overseas
# 7	Non-Governmental Organization	Overseas
# 8	Bank / Money Service Business	Philippines
# 9	Law Enforcement	Philippines
# 10	Bank / Money Service Business	Philippines
# 11	Bank / Money Service Business	Philippines
# 12	Bank / Money Service Business	Philippines
# 13	Bank / Money Service Business	Philippines
# 14	Law Enforcement	Philippines
# 15	Regulator	Overseas
# 16	Regulator	Overseas
# 17	Regulator	Overseas
# 18	Bank / Money Service Business	Overseas
# 19	Bank / Money Service Business	Overseas
# 20	Bank / Money Service Business	Overseas
# 21	Bank / Money Service Business2	Overseas
# 22	Regulator	Philippines
# 23	Regulator	Philippines