ecpat

Down to Zero
Fighting sexual exploitation of children

Addressing the Financial Dimensions of Child Sexual Exploitation

Case study: Indonesia

ECPAT International would like to thank all the persons involved in this case study.

ECPAT Indonesia: Ahmad Sofian, Andy Ardian, and Oviani Fathul Jannah

ECPAT International: Salla Huikuri, Sendrine Constant and Karina Padilla.

The project Step Up the Fight Against Sexual Exploitation of Children – Empowering Children and Communities is supported by the Dutch Ministry of Foreign Affairs under Dutch development/foreign policy with Defence for Children - ECPAT Netherlands.

ECPAT International acknowledges the core funding support for its overall organisational objectives from the Swedish International Development Cooperation Agency (Sida) and Oak Foundation.

The opinions expressed in this document belong solely to ECPAT International. Support from these donors does not constitute endorsement of the views expressed.

Suggested citation: ECPAT International. (2026). Addressing the Financial Dimensions of Child Sexual Exploitation. Case Study: Indonesia. Bangkok: ECPAT International

For feedback or suggestions, please contact researchteam@ecpat.org

Published by:
ECPAT International
328/1 Phaya Thai Road, Ratchathewi,
Bangkok 10400, THAILAND.
Phone: +66 2 215 3388 | Email: info@ecpat.org
Website: www.ecpat.org

The project "Step up the Fight Against Sexual Exploitation of Children – Empowering Children and Communities" is supported by the Dutch Ministry of Foreign Affairs under Dutch development/foreign policy with Defence for Children-ECPAT Netherlands.

CONTENT

GLOSSARY

- **Sexual exploitation of children** is defined by the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse as *"[a] child is a victim of sexual exploitation when they involved in a sexual activity in exchange for something (e.g. money or other gains like food, housing, clothing, protection or even the promise of such) received by a third party and/or the perpetrator"*.[1] It is important to note that the definition of sexual exploitation of children overlaps with that of sexual abuse of children. However, it is distinguished by the presence of an additional element of exchange (money, material goods or access to protection or shelter).

- **Technology-facilitated child sexual exploitation and abuse** according to the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, "technology is an increasingly pervasive element in sexual offending against children and it is becoming rare that no technology at all is used at some stage of the preparation, commission, or further dissemination (in the case of child sexual abuse material) of the sexual exploitation or sexual abuse of a child. Although not always used to facilitate or commit a sexual crime, the overarching role of technology in facilitation means that it can cover crimes committed in both digital and non-digital environments. Firstly, a sexual offence committed in the digital environment is, by definition, facilitated by technology. Secondly, a broad variety of sexual offences committed in-person are made possible with the help of technology, for instance, to connect perpetrators of sexual offences, exchange information, and coordinate actions."[2]

- **Financial typology or red flags:** A description of financial patterns, behaviours, or indicators associated with illicit activities, used to support the detection, prevention, and investigation of crimes. In the context of the sexual exploitation of children, financial typologies help identify warning signs in transactions or financial activities that may be linked to these offences.

1. Interagency Working Group on Sexual Exploitation of Children. (2025). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Thailand: ECPAT International.
2. Ibid

EXECUTIVE SUMMARY

Indonesia ranks among the countries with the highest number of CyberTipline reports involving the upload of child sexual abuse material (CSAM). According to the 2024 CyberTipline Report by the National Centre for Missing & Exploited Children, Indonesia recorded 1,450,403 such reports, following India (2,252,528) and the Philippines (1,721,249).[3] Alongside the growing scale of technology-facilitated child sexual exploitation, financial transactions linked to this crime are increasingly conducted through e-wallets, mule accounts, crypto assets, and cross-border transfers, creating new challenges for detection and disruption.

Addressing these financial flows has therefore become a critical component of efforts to disrupt the sexual exploitation of children. This case study examines how Indonesia is developing financial-sector responses to detect, prevent and disrupt financial transactions linked to child sexual exploitation, highlighting emerging promising approaches, partnerships and regulatory efforts and lessons learned for strengthening financial system responses to child sexual exploitation. Indonesia's experience illustrates how financial intelligence frameworks traditionally developed for anti-money laundering can be adapted to address technology-facilitated child sexual exploitation, particularly where crimes involve complex digital payment ecosystems. Indonesia's experience illustrates how financial intelligence frameworks traditionally developed for anti-money laundering can be adapted to address technology-facilitated child sexual exploitatio, particularly where crimes involve complex digital payment ecosystems.

Although the country has a comparatively strong legal and policy framework, integrating financial intelligence systematically into child sexual exploitation investigations remains an evolving process. Important milestones have been achieved, including regional engagement and collective commitment among stakeholders to establish a dedicated task force on child sexual exploitation and financial transactions, signalling growing institutional commitment despite coordination and sustainability challenges.

3. NCMEC. 2024 CyberTipline Reports by Country

For an evidence-led report outlining online sexual exploitation and abuse of children in Indonesia, see ECPAT, INTERPOL, and UNICEF (2022). Disrupting Harm: Indonesia: Evidence and online child sexual exploitation and abuse. Global Partnership and End Violence Against Children.

This case study examines the legal frameworks, institutional processes, and collaboration models shaping Indonesia's emerging "follow-the-money" approach to child sexual exploitation. While linking financial crimes with online child protection is still a relatively new practice, since 2012 sustained advocacy through collaboration between ECPAT Indonesia and the Indonesian Financial Intelligence Unit has strengthened awareness, public–private dialogue, and the development of red flag indicators.

This case study is based on a desk review of reports, academic publications, and policy documents, complemented by in-depth interviews with key stakeholders, participation in selected strategic meetings and conferences, and validation through a multi-stakeholder consultation.

The analysis identifies several priority areas for strengthening financial responses to child sexual exploitation in Indonesia, including improving national risk assessments through enhanced reporting, institutionalising cross-sector coordination and public–private partnerships, addressing technical capacity gaps across key institutions, and strengthening engagement with the crypto sector and emerging financial technologies.

INTRODUCTION

This case study forms part of a broader series developed by ECPAT International under the Finance Against Child Exploitation: A Global Initiative to Mobilise Financial Responses to Child Sexual Exploitation- FACE IT. This initiative seeks to advance learning on how financial systems can be mobilised to detect and disrupt technology-facilitated child sexual exploitation. As financial transactions increasingly underpin exploitative practices—from small-value payments and livestream tipping to crypto-based transactions—understanding how financial institutions can act as critical actors in prevention and disruption has become essential. Financial exchange is not incidental to these crimes; it is structural, and it leaves traces that can be leveraged for detection, investigation, and accountability.

The case study series contributes to a growing evidence base on how financial-sector engagement is evolving across different national contexts. While promising practices are emerging, efforts remain fragmented, context-specific, and often insufficiently documented. By examining country experiences globally, the series aims to identify the institutional configurations, collaboration models, and enabling conditions that allow financial intelligence to be effectively integrated into child protection responses. This aligns with ECPAT's strategic objective to move beyond reactive approaches and embed financial detection and disruption as a core pillar of child protection systems.

Indonesia represents a particularly relevant case within this series. It illustrates how sustained advocacy, institutional engagement, and multi-stakeholder collaboration can gradually shift financial-sector involvement from awareness-raising to operational practice.

.

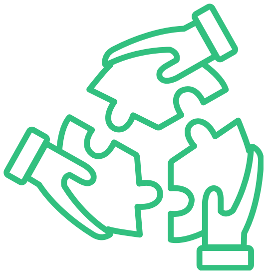
The case highlights how financial intelligence frameworks—traditionally developed for anti-money laundering—can be adapted to address technology-facilitated child sexual exploitation and how red flag indicators, public–private cooperation, and legal innovations can contribute to disrupting exploitation networks. At the same time, it reflects ongoing challenges related to coordination, capacity, and regulatory alignment, offering important lessons for other jurisdictions

By situating Indonesia's experience within a comparative and forward-looking framework, this case study aims to contribute to the development of transferable models for engaging financial institutions in child protection. Ultimately, the series seeks to support the transition from isolated initiatives to systemic, coordinated approaches in which financial detection of child sexual exploitation becomes a standard component of financial governance and child protection architectures globally.

MULTI-STAKEHOLDER RESPONSES

Multi-Stakeholder Collaboration and Coordination

Preventing and disrupting financial flows linked to child sexual exploitation in the financial sector requires coordination across multiple sectors, including financial intelligence authorities, law enforcement, regulatory agencies, financial institutions and financial technology platforms, and civil society organizations.



In Indonesia, the Financial Intelligence Unit has played a central role in convening these actors and developing practical tools to strengthen the financial system's capacity to detect and respond to transactions related to child sexual exploitation.

One key initiative has been the development of red flag indicators for identifying financial transactions potentially linked to the sexual exploitation of children, in collaboration with these multiple stakeholders. This collaborative approach has helped ensure that the indicators reflect both operational realities within financial systems and emerging typologies of financial activity related to sexual exploitation of children.

The Financial Intelligence Unit has also introduced a new public complaint mechanism for cases specific to sexual exploitation of children, expanding the range of actors able to contribute information relevant to financial investigations. Through this mechanism, child protection networks, civil society organisations, regional units for the protection of women and children, and other support institutions can submit complaints or financial information. The Financial Intelligence Unit then applies the 'follow-the-money' analysis to trace and assess suspicious transactions, including cross-checking financial data against multiple national databases. This approach reflects a growing recognition that frontline child protection actors can provide valuable intelligence inputs for financial investigations and demonstrates the growing importance of integrating financial intelligence into child protection responses, allowing authorities to identify organised exploitation networks that may remain invisible through content-based investigations alone.

In parallel, efforts have been made to strengthen capacity within the financial sector itself. ECPAT Indonesia and the Association of Indonesian Financial Transaction Analysts have developed a specialised training module on the misuse of financial technology in child sexual exploitation and related offending. The training targets banks, remittance providers and crypto-asset platforms and has been complemented by awareness-raising activities during National Fintech Month 2025. These initiatives aim to increase financial institutions' ability to recognise emerging financial typologies linked to online child sexual exploitation.

At the policy level, a draft Multi-stakeholder Action Plan has been developed under the Ministry of Women's Empowerment and Child Protection. The plan proposes to establish a dedicated task force under the Coordinating Ministry for Political and Security Affairs to improve inter-agency coordination and address fragmentation in data systems. While the Ministry of Communication and Digital Affairs has strengthened regulatory oversight of digital platforms and operates reporting channels and cyber patrol mechanisms, coordination across ministries remains uneven. Strengthening institutional coordination will therefore be critical to ensure that regulatory, financial intelligence, and child protection responses operate within a coherent national framework.

Financial intelligence efforts are also supported by Indonesia's anti-money laundering framework, which requires financial service providers and virtual asset service providers to submit financial data to the Financial Intelligence Unit through the goAML application[4] when requested. In addition, the Financial Intelligence Unit has begun analysing suspicious transaction patterns linked to child sexual exploitation through a trilateral Financial Intelligence Consultative Group initiative with Malaysia and Singapore, using financial data dating back to January 2020. These cross-border efforts highlight the importance of regional cooperation in addressing financial flows associated with transnational networks of sexual exploitation.

4. The goAML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units and is one of UNODC's strategic responses to financial crime, including money-laundering and terrorist financing. See United Nations Office on Drugs and Crimes, goAML (Anti-Money-Laundering System), https://www.unodc.org/unodc/en/global-it-products/goaml.html.

The Role of the Financial Intelligence Unit in Financial Disruption of child sexual exploitation

Step 1: Detection and Reporting

Suspicious transactions are reported by banks, e-wallet providers, remittance services, and virtual asset service providers through a goAML-application of the United Nations Office on Drugs and Crime. Reports may also originate from law enforcement requests or public complaints. These inputs trigger financial intelligence analysis.

Step 2: Financial Intelligence Analysis

The Financial Intelligence Unit analyses reported transactions using red flag indicators, mapping transaction flows, identifying rapid fund movements or nominee accounts, and cross-checking data against national databases such as population, tax, immigration, and corporate registries to generate actionable intelligence.

Step 3: Intelligence Sharing

Where indicators are confirmed, the Financial Intelligence Unit disseminates financial intelligence to police units, prosecutors, and relevant ministries such as the Ministry of Communication and Digital Affairs.[5] While the Financial Intelligence Unit does not conduct criminal investigations, its analysis supports law enforcement in identifying perpetrators and tracing financial links.

Step 4: Judicial Proceedings

The Financial Intelligence Unit may provide expert testimony in court, explaining transaction flows and money laundering techniques. The integration of anti-money laundering provisions alongside child protection offences enables asset tracing, freezing, and confiscation, strengthening the disruption of exploitation networks.

5. Kementerian Komunikasi dan Digital (Ministry of Communication and Digital Affairs.)

Misused Financial Channels and Transaction Methods

Indonesia demonstrates how financial intelligence can transform child sexual exploitation investigations, shifting from reactive, content-based enforcement to proactive network disruption. Cases of technology-facilitated child sexual exploitation in Indonesia involve a wide range of financial channels, including bank transfers, cards, e-wallets, virtual asset service providers,[6] remittance services, payment gateways, and crypto assets.

Perpetrators exploit both regulated and less regulated providers, often combining digital payments with cash, mobile credit, crypto assets, or cross-border transfers, and using tools such as Virtual Private Networks[7] or the darkweb to conceal identity. Monitoring by ECPAT Indonesia indicates that most cases of technology-facilitated child sexual exploitation are linked to online activities, including child sexual abuse material and livestreamed abuse, with payments commonly made through bank transfers, cash, digital wallets, and in-app rewards on livestreaming platforms. Pricing structures, including per-minute rates for live streaming, demonstrate the commercialised and organised nature of these crimes across social media, messaging apps, gaming platforms, and anonymous forums. These patterns highlight how financial transactions provide critical entry points for detecting child sexual exploitation networks that may otherwise remain hidden within encrypted platforms or closed online communities.

6. Virtual Asset Service Provider (VASP) refers to any business or entity that provides services involving virtual assets (cryptocurrencies or digital tokens)
7. Virtual Private Networks (VPNs) are used to encrypt private internet connections.

Evolution of Indonesia's Financial "Follow-the-Money" Approach

Phase 1: Agenda Setting (2012-2014)

Indonesia's engagement with the financial dimension of child sexual exploitation began in 2012 with the first ASEAN-level conference linking financial technology and online exploitation. Research in 2014 further highlighted connections between child sexual exploitation and financial flows, prompting early engagement between ECPAT Indonesia, the Financial Intelligence Unit and international counterparts. This phase established recognition that financial transactions are central to sexual exploitation networks.

Phase 2: Initial Institutional Engagement (2015-2017)

Under the Down to Zero Alliance, dialogue expanded to include the Financial Intelligence Unit, banks and law enforcement. The financial sector began to be recognised as an important sector in preventing child sexual exploitation, and early discussions emerged around suspicious transaction patterns and red-flag indicators. This marked a shift in cooperation from advocacy towards more operational engagement.

Phase 3: Capacity Development (2018-2020)

The Financial Intelligence Unit strengthened national and regional training within anti-money laundering and countering the financing of terrorism frameworks, while awareness grew that financial flows linked to child sexual exploitation were under-detected. The need for tailored red-flag indicators specific to child sexual exploitation also gained institutional traction.

Phase 4: Legal and Policy Consolidation (2022-2023)

The 2022 Sexual Violence Crimes Law strengthened the criminalisation of technology-facilitated child sexual exploitation. In 2023, President Regulation No. 19/2023 on the National Action Plan for the Prevention and Handling of the Crime of Human Trafficking mandated risk assessments and encouraged the development of red flags and public-private partnerships. Financial disruption became embedded within national child protection policy discussions.

Evolution of Indonesia's Financial "Follow-the-Money" Approach

Phase 5: Institutionalisation of Red Flag Indicators (2023-2025)

Through a trilateral Financial Intelligence Consultative Group project with Malaysia and Singapore (2020–2024), The Financial Intelligence Unit developed structured red flag indicators to help financial institutions detect transactions potentially linked to child sexual exploitation. These indicators were developed through financial data analysis and multi-stakeholder consultation and were launched regionally in 2025 and disseminated nationally, formalising financial typologies for the detection of child sexual exploitation.

Phase 6: Judicial Precedent and Institutional Embedding (2024-2026)

In 2024, the "Premium Place" case became the first to combine Child Protection and Anti–Money Laundering provisions to prosecute an organised network for technology-facilitated child sexual exploitation. The case established financial analysis as a core evidentiary practice. Subsequent developments include a dedicated public complaint mechanism for cases specific cases offor child sexual exploitation, financial-sector awareness campaigns, and discussions on a formal inter-agency task force, further consolidating the system and expanding the range of actors able to contribute information relevant to financial investigations. Moreover, together with a financial analysts' association linked to the Financial Intelligence Unit, ECPAT Indonesia has developed training modules and trained a number of financial service providers to strengthen their understanding of how to prevent child sexual exploitation by addressing the misuse of financial services by offenders.

Taken together, these phases illustrate how responses to child sexual exploitation increasingly require integration between child protection systems, financial intelligence frameworks and digital platform regulation.

Development and Use of Red Flags and Typologies

Financial behaviour often provides earlier signals of child sexual exploitation than content detection, making transaction monitoring an important complementary tool for identifying organised networks of child sexual exploitation.

The Financial Intelligence Unit, accountable to the President of Indonesia, plays a central role in identifying and analysing financial transaction patterns linked to child sexual exploitation.

Through the trilateral Financial Intelligence Consultative Group project with Malaysia and Singapore, the unit developed red flag indicators covering sexual extortion, live-streamed child sexual exploitation, child sexual abuse material, and child sexual exploitation in travel and tourism, based on financial data analysis, surveys, and multi-stakeholder consultations. These indicators were launched in 2025 and are now used as training tools for financial service providers and civil society organisations. Following up on the training program, some providers, such as Bank Central Asia and GoPay (a digital wallet from Gojek, an online transportation platform), have voluntarily integrated these indicators into their monitoring systems, but reportedly have not yet been able to consistently identify suspicious transactions linked to child sexual exploitation. The Financial Intelligence Unit is currently assessing the broader uptake of the red flag indicators among FSPs, but the results had not yet been finalised at the time this case study was developed. Several institutions have indicated that access to a perpetrator watchlist would significantly strengthen their ability to monitor and detect suspicious financial activity.

Examples of Red Flag Indicators Used in Indonesia

The Financial Intelligence Unit developed typologies and red flag indicators through regional trilateral consultation with Malaysia and Singapore. These typologies illustrate how financial behaviour can provide early warning signals of child sexual exploitation networks even when abuse itself occurs on encrypted or closed digital platforms.

Key indicators include:

Sexual extortion of Children
- Repeated small-value payments (1–2 times per week), often late at night
- Use of gift cards, gaming credits, e-wallets, crypto assets
- Rapid movement of funds across multiple short-term accounts
- Cross-border transactions from high-risk jurisdictions
- Payment remarks referencing usernames or nicknames

Live-Streamed Child Sexual Exploitation
- High-frequency micro-payments
- Multiple simultaneous senders
- Immediate withdrawal upon receipt
- Payment remarks such as "support," "gift," or "school fees"
- Escalating payment amounts linked to increasingly exploitative content

Sexual Exploitation of Children in Travel and Tourism
- Airline, hotel, and SIM card purchases in high-risk destinations
- ATM withdrawals in transit or destination countries
- Direct payments to local facilitators

Child Sexual Abuse Material
- Payments to adult platforms, spyware services, or hosting providers
- Negotiated payment amounts
- Multiple unrelated senders
- Online gaming platforms used as payment intermediaries

Reporting, Financial Analysis, and Investigations

Financial transactions increasingly constitute key evidence in investigations and prosecutions of child sexual exploitation. In 2024, the Financial Intelligence Unit reported findings indicating that nearly 24,000 children aged 10-18 years were victims of online sexual exploitation, with associated financial transactions estimated at 127 billion Indonesian rupiah (approximately USD 7.5 million).[8]

These figures illustrate the significant financial dimension of technology-facilitated child sexual exploitation and underscore the importance of integrating financial intelligence into broader investigative responses. When cases are reported by law enforcement, the Financial Intelligence Unit applies a follow-the-money approach, analysing transaction data submitted through the Anti-Money Laundering Reporting and Analysis System (goAML) or other channels. The Financial Intelligence Unit disseminates financial intelligence to law enforcement units, prosecutors, and relevant ministries such as the Ministry of Communication and Digital Affairs. Through this process, financial intelligence is generated and shared to support law enforcement in identifying networks, tracing financial transaction flows, and clarifying the roles of perpetrators and facilitators.

The role of the Financial Intelligence Unit extends beyond financial analysis. It also contributes to criminal proceedings by providing expert testimony and financial analysis in court, thereby strengthening the evidentiary basis for prosecution. The integration of financial intelligence into investigative and judicial processes reinforces law enforcement's capacity to disrupt financial transactions linked to child sexual exploitation and hold perpetrators accountable.

This approach demonstrates how financial intelligence mechanisms developed for anti-money laundering can be leveraged to strengthen responses to technology-facilitated child sexual exploitation, particularly where crimes involve complex digital payment systems and cross-platform transactions.

8. Diana Soraya Noor, Director of Strategy and International Cooperation at PPATK, presented at the ASEAN Conference on the Prevention and Response to the Misuse of Financial Service Providers in Child Sexual Exploitation, Bali, Indonesia, August 2024.

"Premium Place" -case: Applying the Follow-the-Money Approach in Practice

In 2024, Indonesian authorities successfully prosecuted an organised online child sexual exploitation case by combining provisions of the Child Protection Law with Anti-Money Laundering legislation. The case was directly handled by BARESKRIM POLRI in Jakarta, with proceedings taking place in South Jakarta. It demonstrates how financial intelligence can strengthen criminal investigations by tracing financial flows linked to exploitation networks and supporting evidence for prosecution.

Digital Business Model of Sexual Exploitation

The investigation revealed a structured and organised exploitation scheme operating through digital platforms:

- Recruitment of girls under 18 via social media (X/Twitter) and Telegram.
- A structured "membership" system (VIP–VVIP tiers ranging from IDR 500,000–2,000,000)[10]
- Catalogue-based selection of victims marketed as "talent"
- Payments routed through mule accounts and e-wallets

Financial Red Flags Identified

Financial analysis revealed several indicators consistent with organised exploitation:

- Over 2,000 incoming transactions totalling IDR 9.7 billion within a few months.
- High-frequency transactions involving relatively small-value payments.
- Use of third-party nominee accounts.
- Rapid withdrawal and layering of funds.
- Purchase of vehicles registered under other names (to conceal assets).

Judgment and Sentencing

All defendants were found guilty of violations under both the Child Protection Law and the Anti-Money Laundering Law. Sentences ranged from 2 years and 6 months to 4 years imprisonment. In addition, each defendant was fined IDR 5,000,000,000 (approx USD 295,000) with an alternative sentence of six months imprisonment in the event of non-payment.

Legal Significance

- First case adjudicated using both Child Protection and anti-money laundering laws in combination.
- Affirmed that children cannot legally consent to sexual exploitation.
- Established judicial recognition of financial flows as evidence of organised child sexual exploitation.
- Confirmed the use of money laundering techniques such as layering and concealment.

10. Diana Soraya Noor, Director of Strategy and International Cooperation at PPATK, presented at the ASEAN Conference on the Prevention and Response to the Misuse of Financial Service Providers in Child Sexual Exploitation, Bali, Indonesia, August 2024.

"Premium Place" -case: Applying the Follow-the-Money Approach in Practice (continuation)

Impact

Although the case ultimately strengthened prosecution under both the Child Protection Law and the Anti-Money Laundering Law, the role of anti-money laundering analysis extended beyond evidentiary support at trial. Financial intelligence enabled investigators to identify suspicious high-frequency transaction patterns, trace nominee and mule accounts, map the scale and organised structure of the network, and uncover asset purchases made with illicit proceeds. In doing so, financial analysis helped reveal the financial architecture underpinning the exploitation scheme, enabling authorities to better understand the network's operational model.

The case demonstrates how combining child protection legislation with anti-money laundering provisions can strengthen prosecutions of organised child sexual exploitation networks, offering a model that could be replicated in other jurisdictions.

Regional Leadership and International Engagement

Indonesia has positioned itself as a regional leader within ASEAN in addressing the financial dimensions of child sexual exploitation . Early advocacy by ECPAT Indonesia, including a 2012 ASEAN conference that first raised the link between financial technology and child sexual exploitation, helped introduce the issue into regional policy discussions.

More recently, momentum increased significantly between 2023 and 2025, as the Financial Intelligence Unit elevated technology-facilitated child sexual exploitation as a national priority and led a regional study examining suspicious financial transaction indicators associated with child sexual exploitation.

This initiative reflects a growing recognition that financial systems can play a critical role in detecting and disrupting exploitation networks. By leading efforts to identify financial typologies and risk indicators, Indonesia has contributed to strengthening the regional knowledge base on how financial intelligence frameworks can be leveraged to address child sexual exploitation. Indonesia's contribution has also extended globally. The Financial Intelligence Unit has contributed case studies and national insights to the Financial Action Task Force's report on financial flows linked to child sexual exploitation, reinforcing the country's role in shaping emerging international responses to the financial disruption of child sexual exploitation. This engagement highlights the growing intersection between anti-money laundering frameworks and child protection policies at the global level.

Regional collaboration has also been reinforced through multi-stakeholder dialogue. In 2024, ECPAT Indonesia convened the ASEAN Conference on the Misuse of Fintech for Commercial Sexual Exploitation of Children, bringing together financial regulators, law enforcement, financial institutions, and child protection organisations. The conference resulted in the Denpasar Recommendations, supported by the ASEAN Secretariat and various international organisations, which call for stronger cooperation between financial intelligence authorities, regulators, and technology platforms to detect and disrupt financial transactions linked to child sexual exploitation.

Indonesia's experience suggests that financial intelligence units can play a catalytic role in elevating child sexual exploitation within national and regional financial crime agendas, particularly where collaboration between regulators, financial institutions and child protection actors is institutionalised.

ENABLERS AND BARRIERS

Key enablers of success:

Indonesia's regulatory framework has become increasingly victim-centred and child-protective, particularly following the adoption of the Sexual Violence Crimes Law in 2022 and the entry into force of the new Criminal Code in January 2026, which explicitly criminalises multiple forms of technology-facilitated child sexual exploitation. In parallel, the use of anti-money laundering provisions in sexual exploitation cases has further strengthened the legal basis for applying a follow-the-money approach, creating precedents for future prosecutions. While implementation gaps and limited data disaggregation remain challenges, these legal reforms significantly enhance prosecutorial capacity. Overall, these developments illustrate how strengthened legal frameworks can create the enabling conditions for integrating financial investigations into child protection responses.

Institutionally, the Financial Intelligence Unit has also played a central role, supported by professional associations and oversight bodies, and has established a framework for systematically detecting suspicious financial activities. These mechanisms have helped promote institutional continuity and greater transparency through public reporting and the systematic use of red flag indicators to advance the financial disruption of child sexual exploitation

Civil society advocacy and multi-stakeholder engagement have played a critical role in elevating awareness of the financial dimensions of technology-facilitated child sexual exploitation. The efforts of organisations like ECPAT Indonesia and the Down to Zero Alliance have brought the issue onto national and regional policy agendas while facilitating cross-sector collaboration.

Regional platforms such as the 2024 ASEAN Conference and the 2025 Information and Communications Technology Forum have further contributed to greater policy visibility and institutional commitment. Multi-stakeholder trainings have also supported system-building across government, financial institutions, and civil society organisations, helping to expand understanding of financial typologies associated with child sexual exploitation. In parallel, global payment service providers have reinforced internal compliance systems, supporting their Indonesian branches in developing monitoring mechanisms aligned with emerging red flag indicators.

Barriers and structural challenges:

Rapid evolution of digital payment systems is one of the primary challenges in applying financial monitoring approaches to child sexual exploitation. The increasing use of cryptocurrencies, digital tokens, top-up gift cards, e-wallets, and other online payment methods has created new opportunities for perpetrators to obscure financial transactions linked to exploitation. These developments require continuous adaptation of financial monitoring tools, typologies, and regulatory frameworks. Without sustained updates to red-flag indicators and transaction monitoring systems, financial institutions may struggle to keep pace with emerging payment methods used in exploitation networks.

Fragmented coordination and uneven institutional integration remain key challenges in addressing child sexual exploitation. While multiple institutions are involved—including law enforcement, financial intelligence authorities, digital regulators, and child protection agencies—coordination across these actors is still inconsistent. In particular, financial approaches are not yet systematically integrated into child sexual exploitation case management and investigative processes, which continue to focus primarily on victim protection and criminal prosecution. Strengthening coordination between cyber patrol units, law enforcement, financial intelligence authorities, and child protection services will be critical to ensuring that financial investigation becomes a routine component of child sexual exploitation case handling.

Limitations in national risk assessment and data integration remain a key challenge. Within the current National Risk Assessment framework, child sexual exploitation is still classified as a relatively low-risk threat, which may underestimate the scale and financial dimensions of the crime. Child sexual exploitation is widely recognised as a significantly underreported offence due to the vulnerability of victims, social stigma, and coercive control by perpetrators. As a result, available statistics are likely to underrepresent both the prevalence of child sexual exploitation and the associated financial flows.

Information held by victim support organisations and protection services—including insights into exploitation patterns, payment arrangements, and digital platforms used by offenders—is rarely integrated into financial intelligence analysis. Consequently, potentially valuable intelligence remains disconnected from financial monitoring systems. Strengthening cooperation between victim support providers and the Financial Intelligence Unit could improve the detection of suspicious financial transactions linked to exploitation. Integrating victim-related intelligence into financial analysis could also support the development of more targeted red-flag indicators and contribute to reassessing the risk classification of child sexual exploitation within national risk assessment frameworks.

LESSONS LEARNED

The research conducted for this case study identified several institutional challenges related to navigating complex governance structures and influencing policy processes. This underscores the importance of building earlier and stronger collaborations with national and international civil society organisations to enhance collective advocacy leverage, as well as developing coordinated strategies capable of generating the political momentum needed to advance financial-sector responses to child sexual exploitation.

The role of formal institutional mandates in activating financial intelligence mechanisms is also critical. In several instances, the absence of formal ministerial requests to the Financial Intelligence Unit limited its ability to initiate financial analysis related to child sexual exploitation cases. This highlights the extent to which financial intelligence systems remain dependent on political will and formal procedural mandates to operate effectively.

A further structural constraint relates to the legal treatment of predicate offences under Indonesia's Anti-Money Laundering Law (Law No. 8 of 2010). Under the current framework, money laundering charges require prosecutors to demonstrate that assets originate from a specified underlying offence. However, child sexual exploitation is not explicitly listed as a predicate crime. In practice, this means that financial transactions related to child sexual exploitation often need to be linked to other offences—such as human trafficking, prostitution, or violations under the Pornography Law or the Electronic Information and Transactions Law—in order to pursue financial investigations. The absence of explicit recognition of child sexual exploitation as a predicate offence can complicate the classification of suspicious transactions and may limit the ability of financial service providers to identify and report such activity within existing reporting categories.

Operational capacity also remains uneven, affecting the implementation of financial monitoring approaches. Both financial service providers and law enforcement agencies have indicated the need for continued training to strengthen the detection and reporting of suspicious transactions and to apply financial investigation techniques more systematically. In addition, effective detection depends not only on the development of red-flag indicators but also on access to reliable intelligence sources, including legally protected watchlists or databases of perpetrators and associated accounts.

The experience in Indonesia demonstrates that the development of technical tools—such as red-flag indicators and financial monitoring systems—alone is insufficient without sustained political engagement and institutional alignment. While technical solutions are essential for detecting suspicious transactions, their operational impact depends on clear mandates, inter-agency cooperation, and political commitment across relevant institutions. This highlights that financial disruption strategies require not only technical tools but also sustained institutional coordination and political prioritisation.

While the findings presented in this case study are grounded in Indonesia's experience, many of the identified challenges and enabling factors are relevant for other jurisdictions seeking to address the financial dimensions of child sexual exploitation. The case illustrates how financial intelligence frameworks, public–private cooperation, and targeted financial monitoring tools can complement traditional law enforcement approaches to disrupt exploitation networks operating through digital financial systems.

Looking ahead, embedding follow-the-money mechanisms as a standard component of child sexual exploitation investigations, alongside establishing a dedicated inter-agency task force, would be key steps to strengthen coordination, address recidivism, and institutionalise financial disruption strategies.

RECOMMENDATIONS

To establish a state-embedded and sustainable system for preventing and eradicating child sexual exploitation through financial transaction monitoring in Indonesia, the following strategic actions are recommended. While these recommendations are grounded in the Indonesian context, many of the institutional and regulatory challenges identified are common across jurisdictions seeking to address the financial dimensions of technology-facilitated child sexual exploitation.

Strengthen Risk Assessment through Improved Reporting and Data Integration

Indonesia's current national risk assessment classifies child sexual exploitation as a relatively low-risk threat, largely due to limited reporting by financial service providers and the public, reflecting insufficient awareness and the limited integration of victim-related intelligence into financial monitoring systems. Strengthening linkages between victim service providers and the complaint mechanism of the Financial Intelligence Unit dedicated to child sexual exploitation would enhance both the quality and volume of reporting. Integrating these data sources into national risk assessments would provide a more accurate understanding of the scale and financial dynamics of child sexual exploitation.

Institutionalise Cross-Sector Coordination and Public-Private Partnerships

A dedicated cross-stakeholder coordination desk or task force on child sexual exploitation under the Coordinating Ministry for Political and Security Affairs is needed to consolidate inter-agency collaboration. This would support proactive financial tracing, strengthen integration with cyber patrol initiatives, and support more coordinated data-driven enforcement strategies.

In parallel, a structured public–private partnership mechanism should be established to enhance information sharing, regulatory oversight, follow-the-money investigations, capacity building, and international cooperation, with systematic engagement between the Financial Intelligence Unit and reporting entities.

Strengthen Legal Frameworks to Enable Systematic Financial Investigations

Indonesia's anti-money laundering framework currently requires money laundering cases to be linked to a specified predicate offence, yet child sexual exploitation is not explicitly recognised as one under the anti-money laundering law. Clarifying the legal treatment of child sexual exploitation within the anti-money laundering framework would facilitate the systematic application of financial investigations in exploitation cases and improve the ability of financial institutions to classify and report suspicious transactions linked to child sexual exploitation.

Close Technical Capacity Gaps across Key Institutions

Significant capacity gaps persist, particularly in the technical skills required to identify, analyse, and substantiate financial transactions related to child sexual exploitation. Comprehensive and sustained training programmes are needed for financial service providers, law enforcement, and civil society actors to strengthen the detection of suspicious transactions, reporting and the application of financial investigation techniques. Capacity-development efforts should also extend to civil society organisations and victim service providers, enabling them to better identify financial elements of sexual exploitation cases and contribute relevant intelligence to financial investigations. This should be complemented by public education initiatives targeting parents, communities, and children to strengthen prevention and reporting.

Strengthen Monitoring Tools and Intelligence-Sharing Mechanisms

The effectiveness of financial monitoring depends not only on the development of red flag indicators but also on access to reliable intelligence sources. Developing secure and legally compliant information-sharing mechanisms—such as databases or watchlists of known perpetrators, associated accounts, and exploitation-related payment patterns—may significantly improve the ability of financial institutions to detect suspicious transactions.

Engage the Crypto Sector and Leverage Emerging Technologies

The growing use of cryptocurrencies and other digital assets in transactions related to child sexual exploitation underscores the urgency for stronger and more structured engagement with virtual asset services providers, including crypto service providers and regulators. Establishing regulatory guidance and monitoring frameworks for the crypto sector will be essential to prevent exploitation networks from exploiting emerging financial technologies. Integrating AI-based analytical tools and advanced monitoring systems into financial intelligence processes will be critical to strengthen early detection, risk profiling, and disruption of suspicious child sexual exploitation related financial flows.

Tel: +66 2 215 3388
Email: info@ecpat.org
Website: www.ecpat.org