# Enhancing Detection Mechanisms: Law Enforcement Strategies Identifying Suspected Financial Transactions of Child Sexual Exploitation Crimes

Dadang Herli Saputra[1*], Aliyth Prakarsa[2]
[1,2]Fakultas Hukum, Universitas Sultan Ageng Tirtayasa, Serang, Indonesia

dadang.herli@untirta.ac.id

***Abstract.*** *Child sexual exploitation is an increasingly serious issue, exacerbated by the advancement of digital technology, which facilitates undetected financial transactions supporting illegal activities. This study aims to assess and compare the effectiveness of technologies used by Indonesian law enforcement in detecting financial transactions related to child sexual exploitation, with a focus on identifying gaps and proposing solutions. By comparing these methods with those employed in Singapore, the study seeks to provide actionable recommendations for improving Indonesia's capabilities. Using a descriptive-comparative approach, data was collected through literature reviews and analysis of official documents. The findings reveal a significant disparity between the two countries. Singapore has successfully implemented advanced technologies such as predictive analytics and artificial intelligence in its automated transaction monitoring systems, supported by a robust legal framework and effective inter-agency coordination. In contrast, Indonesia faces challenges in adopting technology, lacks high-quality data, and suffers from weak inter-agency coordination. Despite efforts to improve through international cooperation and training, these issues continue to hinder the effectiveness of monitoring systems in Indonesia. The study concludes that enhancing technological adoption, legal frameworks, and inter-agency coordination is crucial for Indonesia to improve its capacity to detect and prevent illegal financial transactions.*

***Keywords****: child sexual exploitation, financial transactions, law enforcement, legal framework, institutional capacity.*

## 1. Introduction

Child sexual exploitation is a critical issue that has intensified with the rapid advancement of digital technology. The use of financial transactions to facilitate these illegal activities is particularly concerning, as perpetrators can now operate more covertly, often using digital money services. The complexity of detecting and preventing such transactions is compounded by numerous technical, legal, and operational challenges.

The International Centre for Missing & Exploited Children (ICMEC) reports that digital technology has broadened the scope of these crimes, complicating efforts to combat them.[1] Furthermore, the Financial Action Task Force (FATF) underscores the necessity of international cooperation and advanced technology to improve the detection and prevention of suspicious financial transactions.[2]

As a developing country, Indonesia faces substantial hurdles in adopting advanced detection technologies. This study aims to assess the effectiveness of the tools and technologies utilized by Indonesian law enforcement agencies in identifying financial transactions related to child sexual exploitation and to compare them with the more advanced

[1]International Centre for Missing & Exploited Children (ICMEC), "Child Sexual Exploitation: An Overview," Alexandria, VA: ICMEC, 2020. [Online]. Available: https://www.icmec.org/. Accessed: Jul. 22, 2024.

[2] Financial Action Task Force (FATF), "Anti-Money Laundering and Counter-Terrorist Financing Measures - Singapore," Paris: FATF-GAFI, 2020. [Online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html. Accessed: Jul. 22, 2024.


A. Sofian et al. (eds.), *Proceedings of the ASEAN Conference on Sexual Exploitation of Children (ACOSEC 2024)*, Advances in Social Science, Education and Humanities Research 876,
https://doi.org/10.2991/978-2-38476-325-2_14

systems employed by Singapore. Singapore's success in implementing sophisticated financial transaction monitoring systems provides a valuable benchmark for Indonesia,[3] which continues to struggle with technological and resource limitations.

Despite global efforts to address financial transactions linked to child sexual exploitation, significant gaps remain, particularly in countries like Indonesia. Singapore's robust legal frameworks, advanced technology, and effective inter-agency coordination enable efficient detection and prevention of such transactions. In contrast, Indonesia's outdated technology, insufficient training, and limited resources hinder its law enforcement capabilities, increasing the risk that many illegal transactions go undetected. This study seeks to identify the challenges and opportunities in implementing detection technologies and offers recommendations to enhance Indonesia's capacity to protect children from sexual exploitation through financial transactions.

## 2. Literature Review

Child sexual exploitation is a grave crime with enduring effects on victims, as perpetrators increasingly exploit financial transactions to support and hide their illicit activities. Recent advancements in digital financial technology have allowed these criminals to conduct transactions with greater sophistication and evasion. The International Centre for Missing & Exploited Children (ICMEC) notes that digital technology has widened the reach of child sexual exploitation, complicating efforts to detect and prevent such crimes.[4]

A particularly concerning tactic is the use of digital currencies and cryptocurrencies, which provide a high level of anonymity, making it difficult for law enforcement agencies to trace the flow of funds. Europol research highlights the growing challenge that cryptocurrencies pose in child sexual exploitation cases, stressing the need for international cooperation and the use of advanced technologies to monitor and track these financial transactions.[5]

Offenders also employ various methods to avoid detection, including the creation of fake accounts and the use of stolen identities to open bank accounts. These evolving tactics underscore the importance of understanding the role of technology in facilitating these crimes and the necessity of enhancing global law enforcement strategies to combat them effectively.

Detecting and preventing financial transactions linked to child sexual exploitation is hindered by technological limitations and insufficient training for law enforcement. The National Institute of Justice (NIJ) notes that many officers lack access to advanced analytical tools and adequate training to identify suspicious transactions.[6] The NIJ emphasizes the need to enhance the capacity and resources available to law enforcement to effectively tackle these issues. In this context, the solution involves not only technological improvements but also international collaboration and effective policy-making. The International Monetary Fund

---

[3] C. H. Lim and J. Goh, "Enhancing Financial Transaction Monitoring through Data Integration and Advanced Analytics in Singapore," *International Journal of Financial Studies*, vol. 9, no. 2, p. 22, 2021.

[4] ICMEC, "*Child Sexual Exploitation: An Overview*," *op. cit.*, [1].

[5] Europol, "*Internet Organised Crime Threat Assessment (IOCTA) 2019*," The Hague: Europol, p. 78, 2019. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf. Accessed: Jul. 22, 2024.

[6] National Institute of Justice (NIJ), "*Challenges and Opportunities in Financial Crime Detection*," Washington D.C.: NIJ, 2020. [Online]. Available: https://nij.ojp.gov/library/publications. Accessed: Jul. 7, 2024.

(IMF) reports that cooperation between nations and global financial institutions is essential to address these challenges.[7]

Detection technologies and instruments for financial crimes have seen significant development in recent years, providing increasingly sophisticated tools for law enforcement to detect and prevent illegal transactions, including those related to child sexual exploitation. Detection technologies, such as Automatic Transaction Monitoring Systems, are crucial in identifying suspicious activities within financial transactions.[8]

These systems employ predefined algorithms and rules to analyze transaction patterns and detect anomalies that may indicate illegal activities. Additionally, financial analytics software like SAS Anti-Money Laundering and IBM Financial Crimes Insight have been widely adopted by financial institutions to improve the identification and reporting of suspicious transactions.[9] Other technologies like blockchain are also increasingly applied in detecting financial crimes, offering transparent and immutable transaction records that aid in tracing the origin of funds and identifying suspicious activities.

## 3. Methodology

This study uses a descriptive-comparative approach to assess the effectiveness of technologies, instruments, and legal systems employed by Indonesian law enforcement in detecting financial transactions related to child sexual exploitation, comparing them with methods in Singapore. Data were collected through a literature review and analysis of official documents, including regulations, policies, and reports from relevant agencies. Content and comparative analyses were applied to evaluate and identify strengths and weaknesses in the systems used by both countries.

To ensure the validity and reliability of the findings, data were triangulated by comparing multiple sources and tested through Focus Group Discussions with legal experts. By utilizing both primary and secondary legal materials, the study aims to develop practical recommendations to improve law enforcement's capacity in Indonesia to detect and prevent financial transactions linked to child sexual exploitation, drawing on successful practices from Singapore.

## 4. Results And Discussion

### 4.1 Legal Framework and Institutional Capacity in Combatting Financial Transactions Related to Child Sexual Exploitation

Combatting child sexual exploitation through financial transactions requires a robust legal framework and institutional capacity to effectively detect, prevent, and prosecute related crimes. In Indonesia, the government has introduced several laws and regulations to address these financial crimes. Evaluating the effectiveness of these laws is crucial to understanding how well the Indonesian legal system can manage this issue, especially in comparison to the more advanced legal frameworks seen in countries like Singapore.

Indonesia's legal efforts include several key laws aimed at detecting and preventing financial transactions linked to child sexual exploitation. Law Number 23 of 2002 on Child Protection, which has been amended multiple times, establishes protections against violence and exploitation. The most recent amendments, such as Law Number 35 of 2014 and Law Number 17 of 2016, increase penalties for perpetrators, underscoring the government's commitment to child protection.

---

[7] International Monetary Fund (IMF). *"Financial Inclusion and Development: Recent Impact and Ongoing Challenges."* Washington D.C.: IMF, 2021.

[8] FATF, *op. cit.*, [2].

[9] S. Sari and A. Rahman, "*The Role of Digital Transactions in Facilitating Illegal Activities in Indonesia,"* Journal of Financial Crime, vol. 28, no. 1, pp. 78-92, 2021.

Additionally, Law Number 21 of 2007 on the Eradication of Human Trafficking specifically addresses trafficking issues, including child sexual exploitation. This law provides a strong legal basis for prosecuting traffickers and protecting victims, while also mandating the monitoring and detection of financial transactions used to facilitate trafficking. Furthermore, to combat money laundering-*a common tactic used by criminals to conceal the proceeds of child sexual exploitation*-Indonesia enacted Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering. This law requires financial institutions to report suspicious transactions to the Financial Transaction Reports and Analysis Center (PPATK), which then conducts further analysis and investigation. These combined legal measures are crucial in Indonesia's efforts to combat financial crimes related to child sexual exploitation, though significant challenges remain in comparison to more developed systems like those in Singapore.

Law Number 11 of 2008 on Information and Electronic Transactions (ITE), which has been amended by Law Number 19 of 2016 and Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008, regulates the use of information technology and electronic transactions in Indonesia. The ITE Law includes provisions to prevent the misuse of technology for illegal activities such as child sexual exploitation. The most recent amendments in Law Number 1 of 2024 introduce stricter provisions regarding data security and privacy in electronic transactions and strengthen mechanisms for reporting and handling suspicious activities. Additionally, this law mandates digital service providers to report suspicious activities that could be used for criminal purposes, assisting law enforcement in detecting and preventing crimes that utilize digital technology.

Moreover, Law Number 27 of 2022 on Personal Data Protection provides a legal framework to protect individuals' personal data, which is particularly important in the context of child sexual exploitation. Personal data protection ensures that sensitive information about victims and investigations is not misused or falls into the wrong hands. By protecting personal data, this law helps maintain the confidentiality and integrity of information used in the investigation and prosecution of child sexual exploitation cases, supporting more effective law enforcement efforts.

On the other hand, Singapore has established a comprehensive legal framework that governs financial transactions related to child sexual exploitation, ensuring the detection, prevention, and prosecution of offenders. This framework is designed to protect children from exploitation, address human trafficking, and prevent money laundering that supports illegal activities. The Children and Young Persons Act (CYPA), enacted in 1993, is a key law that offers extensive protection for children and young people from all forms of violence and abuse, including sexual exploitation. The CYPA sets out provisions to safeguard children from harm and ensures that perpetrators face legal consequences.

To combat human trafficking, Singapore introduced the Trafficking in Persons Act in 2014, which became effective in 2015. This law governs the prevention, prosecution, and protection against human trafficking, including child sexual exploitation. It also includes measures for monitoring and detecting financial transactions that facilitate trafficking, thus strengthening law enforcement against organized crime networks. Additionally, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA), enacted in 1999, plays a crucial role in preventing money laundering, a common method used by criminals to hide the proceeds of their crimes. This law requires financial institutions to report suspicious transactions to authorities, allowing for further investigation and appropriate legal actions to be taken.

The Terrorism (Suppression of Financing) Act (TSOFA), implemented in 2002, prohibits the financing of terrorism and mandates the reporting of suspicious transactions, including those linked to serious crimes like child sexual exploitation. TSOFA strengthens Singapore's legal framework to combat illegal funding that supports various criminal activities. The Personal Data Protection Act (PDPA), which took effect in 2012, governs the protection of personal data in Singapore. In cases of child sexual exploitation, the PDPA

ensures that victims' personal data is safeguarded, maintaining the confidentiality and integrity of sensitive information during investigations and prosecutions.

Additionally, the Prevention of Human Trafficking Act, which became law in 2015, targets human trafficking, including child sexual exploitation, by imposing harsh penalties on traffickers and providing protections and support for victims. Singapore's Penal Code, originally enacted in 1871 and revised multiple times, also contains provisions addressing child sexual exploitation, including penalties for those involved in the production, distribution, or possession of exploitative material. The Code further includes measures to regulate financial transactions that facilitate these crimes, offering a robust legal basis for prosecuting offenders involved in child sexual exploitation.

### 4.2 Technological Support and Implementation Challenges in Law Enforcement

The use of technology in law enforcement is critical in detecting and preventing financial transactions linked to child sexual exploitation. In comparing Indonesia and Singapore, the technological infrastructure and its implementation play a significant role in determining the effectiveness of law enforcement efforts, with noticeable differences between the two countries.

Singapore has developed a highly advanced technological framework that supports its law enforcement agencies in monitoring and analyzing financial transactions.[10] The implementation of sophisticated software such as SAS Anti-Money Laundering and IBM Financial Crimes Insight has allowed Singapore's Commercial Affairs Department (CAD) to process large volumes of data quickly and accurately.[11] These tools use predictive analytics and artificial intelligence (AI) to detect suspicious transaction patterns in real-time, enabling the authorities to respond swiftly to illegal activities. This integration of advanced technology has been crucial in maintaining Singapore's high success rate in preventing financial crimes, including those related to child sexual exploitation.

Moreover, the continuous updates and improvements in Singapore's technological systems ensure that they remain effective against emerging threats. The ability of financial institutions to monitor transactions in real-time and the seamless integration of these systems with law enforcement agencies contribute significantly to the country's effectiveness in combating financial crimes. This advanced infrastructure, coupled with stringent regulatory compliance, positions Singapore as a model for using technology in law enforcement.

In contrast, Indonesia's technological capabilities are still developing. The Financial Transaction Reports and Analysis Center (PPATK) has begun adopting analytical software, but it is generally less advanced compared to Singapore's systems.[12] The technology used by PPATK combines basic analytical techniques with big data processing.[13] However, the lack of advanced features such as AI and predictive analytics limits its effectiveness in real-time detection of suspicious transactions.[14] This technological gap creates challenges in accurately identifying and responding to illegal activities.

One of the major challenges in Indonesia is the inconsistent quality of data available for analysis.[15] Many financial institutions in Indonesia are not yet fully integrated with the automatic transaction monitoring systems,[16] leading to delays and incomplete transaction

---

[10] Monetary Authority of Singapore (MAS). *"Annual Report 2020/2021."* Singapore: MAS, 2021.

[11] S. Sari and A. Rahman, *op. cit.*, [9].

[12] NIJ, *op. cit.*, [6].

[13] Financial Transaction Reports and Analysis Center (PPATK). *Laporan Tahunan PPATK 2021.* Jakarta: PPATK, 2021.

[14] NIJ, *op. cit.*, [6].

[15] Bank Indonesia. *"Financial Stability Review, Second Semester 2021."* Jakarta: Bank Indonesia, 2021.

[16] PPATK, *op. cit.*, [13].

records. This inconsistency in data quality hinders the overall effectiveness of the technology, making it difficult for law enforcement agencies to track and act on suspicious activities. Additionally, the lack of seamless integration between different agencies hampers coordination and data sharing, further reducing the efficiency of financial crime detection.

Operational challenges also play a significant role in the effectiveness of law enforcement technology in both countries. In Singapore, the main challenge is the need for continuous system updates and the refinement of technologies to keep pace with evolving criminal tactics. This requires significant investment in time and resources to maintain the high standards of technological infrastructure. Ensuring that all stakeholders, including financial institutions, comply with the regulatory framework is also an ongoing effort, requiring regular training and audits.

Indonesia faces more foundational challenges in its technological implementation. A significant issue is the lack of adequate training for law enforcement personnel in using these technologies effectively.[17] Advanced software is only as effective as the ability of its users to interpret and act on the data it generates.[18] Unfortunately, many officers in Indonesia do not have access to the necessary training or tools to fully leverage the available technology, resulting in its underutilization and a less effective response to financial crimes related to child sexual exploitation.

Another critical challenge in Indonesia is the limited financial resources available to adopt and maintain cutting-edge technology.[19] The high costs associated with acquiring, implementing, and continuously upgrading these systems are substantial, and budget constraints often limit the ability to invest in the most effective tools. Additionally, the lack of coordination among various law enforcement agencies further hampers the effectiveness of these technologies, as it impedes the sharing of critical information and collaborative efforts needed to combat financial crimes.

This analysis highlights the stark differences in the technological support and implementation challenges faced by law enforcement in Indonesia and Singapore. While Singapore's advanced infrastructure and continuous improvement efforts enable effective detection and prevention of financial transactions related to child sexual exploitation, Indonesia continues to struggle with foundational challenges in technology, training, and resource allocation. Addressing these challenges is essential for enhancing Indonesia's capacity to protect children from exploitation through the financial system.

## 5. Conclusions

The conclusion of this study highlights a significant disparity in the effectiveness of law enforcement in addressing financial transactions related to child sexual exploitation between Indonesia and Singapore. Singapore has successfully implemented advanced technologies such as predictive analytics and artificial intelligence in its automated transaction monitoring systems, enabling the detection of suspicious transactions with a high success rate. The support of a robust legal framework and effective inter-agency coordination also enhances Singapore's law enforcement capacity to efficiently tackle financial crimes related to child sexual exploitation.

Conversely, Indonesia faces significant challenges in adopting advanced technology and resource limitations. Despite efforts to enhance technology through international cooperation and staff training, the lack of high-quality data and inter-agency coordination hampers the effectiveness of its automated transaction monitoring systems. The complex

---

[17] NIJ, *op. cit.*, [6].

[18] National Institute of Justice (NIJ), "*Training for Financial Crime Detection and Analysis,*" Washington D.C.: NIJ, 2020.

[19] United Nations Office on Drugs and Crime (UNODC), "*Indonesia Country Report on Financial Crimes 2021,"* Vienna: UNODC, 2021.

bureaucracy and high levels of corruption within Indonesia's legal system further reduce the consistency of law enforcement. Additionally, many financial institutions in Indonesia still rely on manual systems, which diminishes the early detection effectiveness of suspicious transactions.

## REFERENCES

[1] Bank Indonesia. *Financial Stability Review*, Second Semester 2021. Jakarta: Bank Indonesia, 2021.
[2] C. H. Lim and J. Goh, *"Enhancing Financial Transaction Monitoring through Data Integration and Advanced Analytics in Singapore,"* International Journal of Financial Studies, vol. 9, no. 2, p. 22, 2021.
[3] Europol, *"Internet Organised Crime Threat Assessment (IOCTA) 2019,"* The Hague: Europol, p. 78, 2019. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf. Accessed: Jul. 22, 2024.
[4] Financial Action Task Force (FATF), *"Anti-Money Laundering and Counter-Terrorist Financing Measures - Singapore,"* Paris: FATF-GAFI, 2020. [Online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html. Accessed: Jul. 22, 2024.
[5] Financial Transaction Reports and Analysis Center (PPATK). *Laporan Tahunan PPATK 2021*. Jakarta: PPATK, 2021.
[6] International Centre for Missing & Exploited Children (ICMEC), *"Child Sexual Exploitation: An Overview,"* Alexandria, VA: ICMEC, 2020. [Online]. Available: https://www.icmec.org/. Accessed: Jul. 22, 2024.
[7] International Monetary Fund (IMF). *Financial Inclusion and Development: Recent Impact and Ongoing Challenges*. Washington D.C.: IMF, 2021.
[8] Monetary Authority of Singapore (MAS). *Annual Report 2020/2021*. Singapore: MAS, 2021.
[9] National Institute of Justice (NIJ), *"Challenges and Opportunities in Financial Crime Detection,"* Washington D.C.: NIJ, 2020. [Online]. Available: https://nij.ojp.gov/library/publications. Accessed: Jul. 7, 2024.
[10] National Institute of Justice (NIJ), *"Training for Financial Crime Detection and Analysis,"* Washington D.C.: NIJ, 2020.
[11] S. Sari and A. Rahman, *"The Role of Digital Transactions in Facilitating Illegal Activities in Indonesia,"* Journal of Financial Crime, vol. 28, no. 1, pp. 78-92, 2021.
[12] United Nations Office on Drugs and Crime (UNODC), *"Indonesia Country Report on Financial Crimes 2021,"* Vienna: UNODC, 2021.