


Know Your Customer (KYC) Model: A Legal Reform Strategy to Prevent Abuse of Financial Services in Child Sexual Exploitation Transactions

**Zentoni ^a✉, Budi Santoso ^a, David M. L. Tobing ^a,
Zico Junius Fernando ^b **

^a Faculty of Law, Universitas Diponegoro, Indonesia

^b Faculty of Law, Universitas Bengkulu, Indonesia

✉ corresponding email: zenlaw79@gmail.com

Abstract

KYC (Know Your Customer) is a process undertaken by financial institutions to identify and verify the identity of their customers. The aim is to prevent financial crimes such as money laundering, fraud and terrorist financing. This Know Your Customer (KYC) model can be used as a strategic framework for financial institutions to prevent misuse of financial services including child sexual exploitation transactions that are rampant. The model emphasizes rigorous customer identification, verification and continuous monitoring of transactions to detect suspicious activity. By carefully understanding customer financial behavior, financial institutions can identify anomalies that may indicate illicit activities, including those related to child exploitation. Globally, financial service providers including major banks such as HSBC, JPMorgan Chase, and Citigroup, as well as digital payment platforms such as PayPal and Stripe exemplify and can play a key role in preventing child sexual exploitation.

This research uses normative legal research methods. The nature of this research is descriptive-prescriptive. The result of this research states that in the future, financial institutions can implement strict KYC (Know Your Customer) policies, monitor suspicious transactions, and cooperate with law enforcement agencies from various countries. This comprehensive approach not only helps combat child exploitation, but also improves global regulatory compliance, thus maintaining the integrity of the financial system. The implementation of the KYC model involves collaboration with law enforcement and utilizes advanced technology for efficient data analysis and customer monitoring. Ultimately, this model serves to protect vulnerable populations while upholding ethical standards within the financial sector.

Keywords

KYC; Financial Institutions; Child Sexual Exploitation; Transaction Monitoring; Suspicious Activities.

Introduction

Child sexual exploitation is one of the most horrifying crimes that violates human rights, morality, and fundamental values of humanity. Every year, millions of girls and boys worldwide fall victim to sexual violence and exploitation.¹ This crime knows no geographical boundaries, occurring in every country and across all layers of society, from remote communities to advanced urban centers.² More than just a criminal act, child sexual exploitation leaves long-term impacts that devastate the lives of victims, including psychological trauma, social marginalization, and developmental disruptions. This phenomenon poses a serious threat to the future of younger generations and reflects a collective failure to protect the fundamental rights of children.³ A child

¹ Josenhans, Valentine, et al. "Gender, rights and responsibilities: The need for a global analysis of the sexual exploitation of boys." *Child Abuse & Neglect* 110 (2020): 1–7, <https://doi.org/https://doi.org/10.1016/j.chiabu.2019.104291>.

² Jonathan, Okpuvwie Ejuvweyere, et al. "Impacts of crime on socio-economic development." *Mediterranean Journal of Social Sciences* 12.5 (September 5, 2021): 71–81, <https://doi.org/10.36941/mjss-2021-0045>.

³ Simon, June, Ann Luetzow, and Jon R. Conte. "Thirty years of the convention on the rights of the child: Developments in child sexual abuse and exploitation." *Child abuse & neglect* 110 (2020): 1–5, <https://doi.org/https://doi.org/10.1016/j.chiabu.2020.104399>.

can become a victim of sexual violence or exploitation at home, in school, or within their community.⁴ The widespread use of digital technology can also put children at risk. More often than not, the violence is committed by someone the child knows and trusts.⁵

At least 120 million girls under the age of 20, or roughly 1 in 10, have experienced forced sexual acts, such as being coerced into sex or other sexual activities. This figure is likely an underestimation due to the widespread stigma and fear associated with reporting such crimes.⁶ Among those who report these experiences, approximately 90 percent of adolescent girls state that their first perpetrator was someone they personally knew.⁷ In many cases, this individual is identified as a boyfriend, partner, or husband. Additionally, there is a significant gap in data regarding victims who remain silent. Millions of boys and other survivors of sexual violence choose not to share their experiences, leaving much of the issue hidden from public awareness and official records.⁸

This crime not only results in deep physical and psychological suffering for the victims but also undermines social order and public trust in the legal system and the enforcement of justice. In this era of globalization and digitalization, these crimes have become increasingly difficult to detect and eradicate because perpetrators can exploit technology and financial services to cover their tracks. The internet and social media have become the primary tools for offenders to access and exploit victims, whether through psychological manipulation, blackmail, or coercion. Additionally, digital financial services allow perpetrators to

⁴ *Ibid.*

⁵ Pendergast, Kirra. "Protecting Children Online: Strategies for a Safer Future." *Ubiquity Proceedings* 3.1 (June, 2023): 334–39, <https://doi.org/10.5334/uproc.105>.

⁶ Stamatakis, Caroline E., et al. "Sexual violence prevalence and related pregnancy among girls and young women: a multicountry analysis." *Journal of interpersonal violence* 37.3–4 (2022): NP2428–NP2441, <https://doi.org/10.1177/0886260520936366>.

⁷ Barbara, Giusy, et al. "Sexual violence against adolescent girls: labeling it to avoid normalization." *Journal of Women's Health* 26.11 (2017): 1146–1149, <https://doi.org/10.1089/JWH.2016.6161>.

⁸ Anubhab Mukherjee, "Silent Suffering: The Unspoken Reality of Male," *International Journal of Research and Review* 11, no. August (2024): 613–24, <https://doi.org/https://doi.org/10.52403/ijrr.20240866>.

conduct anonymous transactions, trade child sexual exploitation content, and facilitate transnational human trafficking networks. Recently, Indonesia's Financial Transaction Reports and Analysis Center (PPATK) uncovered financial transactions worth Rp 114 billion linked to human trafficking and child pornography. This discovery was made by tracking banking activities. PPATK reported that many child sexual exploitation offenders use digital wallets or e-wallets for sexual payments. This finding is alarming as it shows that children are being sold for sexual purposes in significant numbers.⁹

Perpetrators of child sexual exploitation crimes have utilized financial institutions to carry out financial transactions. Financial institutions are deliberately exploited to obscure the origin of the money. Furthermore, with the rapid development of information and technology, online transactions have also become more common.¹⁰ There is a global and national trend where perpetrators of child sexual crimes use payment methods involving non-bank financial institutions. Examples include money transfer services, transactions through e-wallets, or other forms of financial transactions that are difficult to detect by the Financial Transaction Reports and Analysis Center (PPATK). Thus, offenders can more easily make payments and receive the proceeds of their crimes anonymously, complicating law enforcement efforts to trace and stop these illegal activities. One effort that can be implemented is the use of Know Your Customer (KYC), a strategy used by financial institutions to identify and verify the identities of their customers.¹¹ The main purpose of the KYC process is to prevent financial crimes such as money laundering, fraud, and terrorist financing. However, the potential of KYC to prevent the misuse of financial services for transactions related

⁹ Adrial Akbar, "PPATK Temukan Transaksi Rp 114 M Terkait Pornografi Anak Selama 2022," detikNews, 2022, <https://news.detik.com/berita/d-6485840/ppatk-temukan-transaksi-rp-114-m-terkait-pornografi-anak-selama-2022>.

¹⁰ Cubitt, Timothy IC, et al. "Understanding the offline criminal behavior of individuals who live stream child sexual abuse." *Journal of interpersonal violence* 38.9-10 (2023): 6624-6649, <https://doi.org/10.1177/08862605221137712>.

¹¹ Jain, Harsh, et al. "Financial investment recommendation and decentralized account management." *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, (2020): 1-6, <https://doi.org/10.1109/ICCCNT49239.2020.9225326>.

to child sexual exploitation can be further optimized and more effectively implemented. A strict KYC model can serve as a strategic framework for financial institutions to prevent the misuse of financial services, including the rampant child sexual exploitation transactions.

Method

This study aims to explore how the strategic implementation of the *Know Your Customer* (KYC) model can prevent the abuse of financial services in transactions related to child sexual exploitation. The research uses a normative approach, focusing on the legal frameworks, principles, and regulatory policies underpinning the KYC system, and how these can be strengthened or adapted to address specific crimes such as child sexual exploitation.¹² Normative research is a legal research method aimed at understanding and analyzing law as a norm or a set of rules that are in force.¹³ In the context of financial services, child sexual exploitation often involves transactions that attempt to obscure the flow of money used for illegal activities, such as the trafficking of child sexual abuse material or the trafficking of children for sexual purposes. Criminals often exploit gaps in financial systems by using anonymous or untraceable transactions to evade detection. Therefore, a robust KYC model is crucial in identifying, monitoring, and mitigating the risks of financial system abuse for such purposes. Through a normative approach, this study highlights the legal dimensions of KYC, examining the existing regulations and guidelines, both nationally and internationally, that govern the application of KYC, and how these obligations are tied to broader *Anti-Money Laundering* (AML) and *Counter Terrorist Financing* (CTF) regulations. The study also identifies gaps in the current legal framework that allow for the misuse of financial systems by those involved in child sexual exploitation transactions. Additionally, the

¹² Fernando, Zico Junius, et al. "The Role of Neuroprediction and Artificial Intelligence in the Future of Criminal Procedure Support Science: A New Era in Neuroscience and Criminal Justice." *Yuridika* 38.3 (2023): 593-620, <https://doi.org/10.20473/ydk.v38i3.46104>

¹³ Widyawati, Anis, et al. "Urgency of the Legal Structure Reformation for Law in Execution of Criminal Sanctions." *Lex Scientia Law Review* 6.2 (2022): 327-358, <https://doi.org/10.15294/lesrev.v6i2.58131>

study evaluates the core processes of the KYC model, such as the *Customer Identification Program* (CIP) and *Customer Due Diligence* (CDD), and how these elements can be legally mandated and enforced to prevent transactions related to child sexual exploitation. Through normative analysis, this research also investigates the role of *Enhanced Due Diligence* (EDD) in high-risk situations and examines the evolution of e-KYC technologies, such as biometric verification and artificial intelligence (AI), from a legal perspective.

Result and Discussion

A. Enhancing Legal Frameworks for KYC: A Strategic Response to Combat Financial Exploitation in Child Sexual Crimes

The Know Your Customer (KYC) model is a fundamental cornerstone in the financial industry, designed to ensure that companies understand the identity, background, and potential risks associated with their customers.¹⁴ This process involves the collection of relevant personal information, such as full name, address, date of birth, and official identification (such as ID cards, passports, or driver's licenses), and often includes background checks to ensure that prospective customers are not involved in illegal activities such as money laundering, terrorist financing, or fraud. KYC is also used to comply with anti-money laundering (AML) and Counter Terrorist Financing (CTF) regulatory standards set by national and international financial oversight bodies. The KYC model consists of several important stages.¹⁵ First, the Customer Identification Program (CIP), in which companies are required to identify and verify the identity of customers using official documents. Second, Customer Due Diligence (CDD), which involves a

¹⁴ Nilsson, Johan. "Know your customer: Client captivation and the epistemics of market research." *Marketing Theory* 19.2 (2019): 149-168, <https://doi.org/10.1177/1470593118787577>.

¹⁵ Krist, By Marcel. "Will Financial Institutions Ever Achieve a 100% Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Rules?." *The RegTech Book* (2019), <https://doi.org/10.1002/9781119362197.CH30>.

deeper analysis of the customer's risk profile, including the source of funds and the purpose of the transactions. This stage is crucial for understanding whether a customer may be involved in suspicious activities. Lastly, Enhanced Due Diligence (EDD) refers to additional procedures applied to customers deemed high risk, such as politically exposed persons or individuals involved in large, unusual transactions. Furthermore, KYC is not only performed at the initial stage when a business relationship is established but must also be continuously applied through ongoing transaction monitoring. Companies must be able to detect transactions that do not align with the previously identified customer profile. For example, if a customer suddenly engages in unusually large transactions or dealings with high-risk countries, the company must conduct further investigations. In the digital era, the KYC model has also evolved. Many companies now adopt e-KYC, which uses technologies such as biometric verification, facial recognition, and artificial intelligence (AI) analytics to expedite and improve the accuracy of customer verification processes. This is essential for addressing the challenges posed by increasingly complex digital transactions that are vulnerable to cybersecurity threats. Effective KYC implementation not only helps companies comply with regulations and avoid legal sanctions but also enhances public trust in financial institutions. By mitigating the risks of financial crimes, KYC helps maintain the overall stability of the financial system.

The development of a legal framework for Know Your Customer (KYC) in the context of preventing the abuse of financial services in transactions related to child sexual exploitation is one of the major challenges facing the global banking and financial services system today. Child sexual exploitation, especially involving financial transactions, is often carried out through non-transparent financial channels, where perpetrators attempt to obscure the source or destination of funds to avoid detection. In this regard, a KYC model designed to identify, monitor, and mitigate these risks must be supported by a robust legal framework integrated with strategic approaches to effectively combat child sexual exploitation.

The legal framework supporting the implementation of KYC must be grounded in legal principles directly related to child protection, anti-

money laundering (AML), and counter-terrorist financing (CTF).¹⁶ Currently, AML and CTF regulations serve as the foundation for KYC requirements in various jurisdictions. However, the emphasis on child sexual exploitation in relation to financial transactions has not been fully integrated into existing KYC regulations. One critical legal approach in developing this framework is the application of more comprehensive Customer Due Diligence (CDD) to identify customer risks. As part of a stronger legal strategy, regulations could mandate stricter scrutiny of suspicious transactions, especially when there are indications that funds are being used for crimes related to child sexual exploitation. For instance, in the UK, the Financial Conduct Authority (FCA) has emphasized the importance of deeper transaction monitoring to identify illegal financial activities linked to serious crimes, including child exploitation. This legal framework also needs to integrate a human rights protection approach, particularly children's rights, as a core principle in KYC regulation. Based on the Convention on the Rights of the Child (CRC), states are obliged to protect children from all forms of sexual exploitation and child trafficking. Countries that have ratified this convention are required to enforce laws that ensure the protection of children from all forms of crime, including through financial channels.

The development of a KYC legal framework focused on preventing child sexual exploitation can be analyzed through several relevant legal theories. Legal compliance theory posits that the law must create mechanisms that compel financial institutions to adhere to strong KYC policies. According to this theory, severe legal penalties for KYC violations can serve as a strong incentive for financial institutions to comply with these regulations. For example, imposing heavy penalties on financial institutions that fail to detect suspicious transactions related to child exploitation can be an effective deterrent. Additionally, the theory of legal protection can be applied, whereby the state is obligated to create a legal system that protects vulnerable parties, including children, from sexual exploitation. This protection should include KYC regulations that

¹⁶ See, Benedictus Renny, and Ahmadi Miru. "Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes." *JL Pol'y & Globalization* 81 (2019): 101, <https://doi.org/10.7176/JLPG>.

require financial institutions to take more effective preventive and monitoring measures. To develop an effective legal framework, it is important to examine real-world examples where financial services abuse has occurred in the context of child sexual exploitation. One relevant case is the Backpage case, where a website was seized by the U.S. government for facilitating child trafficking for sexual purposes. One of the key findings in this case was how child traffickers used online payment systems and cryptocurrencies to avoid detection. In this case, the lack of KYC oversight on the financial services used by the perpetrators was a gap that was exploited. This case highlights the importance of developing a legal framework that explicitly mandates that digital financial services and payment platforms comply with strict KYC requirements, particularly when there is a risk of child sexual exploitation. Increasing legal obligations, including deeper scrutiny of cryptocurrency use and anonymous transactions, must be a top priority in the legal framework that needs to be developed.

Proposed legal reforms in developing the KYC framework must include several key aspects. First, there is a need for greater regulatory harmonization across countries concerning KYC, particularly in the international context where child sexual exploitation often involves cross-border networks. Currently, the Financial Action Task Force (FATF) standards provide guidance on the importance of KYC implementation in combating financial crime.¹⁷ However, these standards need to be reinforced with specific regulations addressing child sexual exploitation. Second, legal reforms must also expand the scope of KYC to cover various forms of digital and non-traditional transactions. As technology evolves, financial transactions are becoming increasingly difficult to trace due to the anonymity provided by digital currencies. Therefore, KYC laws must accommodate these developments and require financial institutions to take additional steps in monitoring such transactions. Third, legal reforms must focus on enhancing the capacity of law enforcement to monitor and address transactions related to child sexual exploitation. This includes better training for financial regulators,

¹⁷ Zamina Hasanli, "FATF Recommendations as A Major Tool for AML," *Scientific Research International Online Scientific Journal* 3, no. 4 (2023): 1–23, <https://doi.org/10.36719/2789-6919/20/91-93>.

improved monitoring technology, and the implementation of more effective reporting mechanisms. Training for financial institutions in detecting suspicious transactions related to child sexual exploitation is also a crucial part of these reforms. Additionally, the development of adequate technological infrastructure will ensure that monitoring and detection can be done quickly and efficiently. Through this comprehensive legal approach, the KYC framework can become more effective in preventing the abuse of financial services for child sexual exploitation, providing stronger protection for vulnerable groups, and ensuring that offenders can be detected and prosecuted with appropriate legal action.

B. Integrating Advanced e-KYC Technologies: Legal Innovations to Prevent Child Sexual Exploitation in Financial Transactions

The implementation of electronic Know Your Customer (e-KYC) technology is an innovative step that can enhance identification systems and risk mitigation in financial services, particularly in the context of preventing child sexual exploitation, which often exploits gaps in financial transactions. e-KYC technology relies on artificial intelligence (AI) and biometrics to accelerate, strengthen, and expand the customer identity verification process, enabling more accurate and efficient detection of suspicious activities.¹⁸ This approach is crucial as perpetrators of child sexual exploitation often use hard-to-trace transactions, such as payments through cryptocurrency or anonymous payment services. Integrating advanced technology with a clear and robust legal framework is a key foundation for combating financial crimes related to child sexual exploitation.

e-KYC (Electronic Know Your Customer) technology offers various innovative advantages in enhancing the security and efficiency of customer verification processes while remaining within the context of

¹⁸ Verma, Kavary, et al. "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking." *2023 9th International Conference on Signal Processing and Communication (ICSC)*. IEEE (2023): 319–24, <https://doi.org/10.1109/ICSC60394.2023.10441596>.

preventing financial crimes, including child sexual exploitation. Some of the approaches used in e-KYC include:

1. Biometric Verification

Biometric verification is a technology that utilizes biological and physical characteristics, such as facial recognition, fingerprint scanning, or retina scanning, to uniquely verify an individual's identity.¹⁹ This technology plays a critical role in the *e-Know Your Customer* (e-KYC) process, as biometric data offers a high level of uniqueness and is significantly harder to forge compared to physical documents like ID cards or passports. In facial recognition, the system employs advanced algorithms to map facial features, such as the distance between the eyes or the shape of the cheekbones, which are then matched against data stored in a database. Similarly, fingerprint scanning analyzes the unique patterns on a user's finger, which remain unchanged throughout their lifetime, providing a highly accurate means of identification. Retina or iris scanning further enhances security by examining the intricate patterns in the eye, which are nearly impossible to replicate. This technology not only enhances the security of identity verification processes but also improves efficiency by enabling fast and automated verifications. With these capabilities, biometric verification adds a robust layer of protection in modern financial systems, preventing identity misuse for crimes, including child exploitation in financial transactions.

2. Artificial Intelligence (AI)

Artificial Intelligence (AI) is a cornerstone technology in the implementation of e-KYC, offering the capability to analyze transaction data in real-time with unmatched efficiency. By leveraging advanced algorithms and machine learning models, AI can detect patterns and anomalies within financial transactions that may signal illicit activities, such as human trafficking, money laundering, or the funding of illegal enterprises.²⁰ For instance, AI

¹⁹ Lawton, George. "Biometrics: a new era in security." *Computer* 31.08 (1998): 16-18, <https://doi.org/10.1109/MC.1998.707612>.

²⁰ Sharma, Preeti, A. Shanker Prakash, and Anjul Malhotra. "Application of Advanced AI Algorithms for Fintech Crime Detection." *2024 15th International Conference on Computing Communication and Networking Technologies*

systems are capable of recognizing unusual transaction behaviors, such as frequent transfers of small amounts to multiple accounts or sudden large transactions from accounts that typically show minimal activity.²¹ These capabilities allow AI to flag activities that deviate from established customer profiles, providing a critical tool for identifying suspicious behavior that might otherwise go unnoticed.²² Moreover, with its ability to process vast volumes of data at high speed, AI can monitor thousands of transactions simultaneously, ensuring continuous vigilance over financial networks.²³ This capability is particularly crucial in combating crimes such as child sexual exploitation, where perpetrators often attempt to hide their activities through complex or fragmented financial flows. By automating the detection process, AI reduces the reliance on manual monitoring, enabling faster responses to potential threats while enhancing the overall effectiveness of financial compliance systems.

3. Reduced Reliance on Physical Documents

Reduced reliance on physical documents is a significant advantage of e-KYC, as it allows financial institutions to move away from traditional methods of identity verification that rely on physical documents, which are often susceptible to forgery or tampering. Instead, e-KYC enables digital verification processes, leveraging advanced technologies such as biometric data, secure digital signatures, and encrypted databases. This shift not only minimizes the risk of identity fraud but also streamlines the customer onboarding process, making it faster and more efficient. Customers can now verify their identities remotely without the

(*ICCCNT*). IEEE, (2024): 1-6, <https://doi.org/10.1109/ICCCNT61001.2024.10725857>.

²¹ Kingdon, Jason. "AI fights money laundering." *IEEE Intelligent Systems* 19.3 (2004): 87-89, <https://doi.org/10.1109/MIS.2004.1>.

²² Legg, Philip A., et al. "Automated insider threat detection system using user and role-based profile assessment." *IEEE Systems Journal* 11.2 (2015): 503-512., <https://doi.org/10.1109/JSYST.2015.2438442>.

²³ Alahira, Joshua, et al. "The role of artificial intelligence in enhancing tax compliance and financial regulation." *Finance & Accounting Research Journal* 10 (2024): 241–251, <https://doi.org/10.51594/FARJ.V6I2.822>.

need to present physical documents in person, which is particularly beneficial for enhancing accessibility to financial services in rural or underserved areas.²⁴ Additionally, digital verification ensures a more secure storage and transfer of identity data, reducing the likelihood of data breaches or unauthorized access compared to traditional document handling methods. By eliminating the dependency on physical documents, e-KYC significantly improves the integrity, security, and efficiency of identity verification processes in the financial sector.

4. Cross-Border Transaction Monitoring

Reduced reliance on physical documents is a significant advantage of e-KYC, as it allows financial institutions to move away from traditional methods of identity verification that rely on physical documents, which are often susceptible to forgery or tampering.²⁵ Instead, e-KYC enables digital verification processes, leveraging advanced technologies such as biometric data, secure digital signatures, and encrypted databases. This shift not only minimizes the risk of identity fraud but also streamlines the customer onboarding process, making it faster and more efficient.²⁶ Customers can now verify their identities remotely without the need to present physical documents in person, which is particularly beneficial for enhancing accessibility to financial services in rural or underserved areas. Additionally, digital verification ensures a more secure storage and transfer of identity data, reducing the likelihood of data breaches or unauthorized access compared to traditional document handling methods. By eliminating the dependency on physical documents, e-KYC

²⁴ Perlman, Leon, and Nora Gurung. "Focus note: the use of eKYC for customer identity and verification and AML." *Available at SSRN 3370665* (2019): 1–28, <https://doi.org/10.2139/SSRN.3370665>.

²⁵ Verma, Kavery, et al. "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking." *2023 9th International Conference on Signal Processing and Communication (ICSC)*. IEEE, 2023.

²⁶ Chakraborty, S., et al. "E-KYC system using blockchain." *International Journal for Research in Applied Science and Engineering Technology* 11.7 (2023): 1174-1181, <https://doi.org/10.22214/ijraset.2023.54834>.

significantly improves the integrity, security, and efficiency of identity verification processes in the financial sector.

Through these approaches, e-KYC technology plays a crucial role not only in preventing and combating financial crimes, including those related to child sexual exploitation, but also in advancing consumer protection by fostering a secure and trustworthy financial environment. By offering a faster, more secure, and highly accurate verification process, e-KYC minimizes the risk of identity fraud, ensuring that consumers' personal and financial information remains safeguarded. This digital transformation enhances the confidence of consumers in financial institutions, as they can be assured that their data is protected against misuse or unauthorized access. Moreover, the implementation of e-KYC aligns with the principles of consumer protection by enabling financial institutions to identify and address fraudulent activities early, thereby reducing the likelihood of consumers falling victim to scams or financial exploitation. For instance, the capability of e-KYC systems to detect anomalies in transaction patterns not only disrupts criminal networks but also protects consumers from being unknowingly involved in suspicious or illegal transactions. This proactive approach prevents potential financial harm to consumers, such as unauthorized charges or fraudulent withdrawals.

With the advancement of e-KYC technology, stricter monitoring of suspicious transactions has become easier. Artificial intelligence can monitor and learn the normal transaction behavior of a customer, and when a deviation occurs, such as a large transaction that does not match the customer's profile, the system automatically alerts the financial institution to conduct further investigation. This is crucial in preventing the misuse of financial services by perpetrators of child sexual exploitation, who often attempt to manipulate the system through unusual transaction patterns but remain in small amounts to avoid manual detection.

In the legal context, the implementation of e-KYC requires clear regulatory adjustments to ensure that financial institutions can fulfill their obligations in using this technology, particularly to prevent child sexual exploitation. Technologies such as biometrics and artificial intelligence (AI) used for identity verification and transaction

monitoring introduce new legal challenges, especially regarding data privacy protection and system accuracy. Regulations must pay special attention to the aspect of personal data security, adopting international standards such as the General Data Protection Regulation (GDPR) applicable in the European Union. GDPR sets strict guidelines on how biometric data is collected, stored, and used by financial institutions. This is crucial given the increasing risks of data breaches or misuse of sensitive information as the use of advanced technologies grows. Moreover, the law should explicitly regulate the liability of financial institutions in the event of violations or failures in e-KYC implementation. For example, in cases where child sexual exploitation goes undetected due to weaknesses in the e-KYC system, financial institutions should be held legally accountable. This requires clarity in laws regarding sanctions for institutions that fail to meet their obligations according to established standards. Such regulations are essential to ensure that the use of e-KYC technology is not only effective in preventing crimes but also capable of protecting individual rights, particularly in terms of data privacy and security.

The implementation of e-KYC (electronic Know Your Customer) has rapidly advanced in many countries around the world, with each country adopting different approaches depending on its legal framework and technological readiness. e-KYC allows financial institutions to digitally verify customer identities, utilizing technologies such as biometrics and artificial intelligence (AI) to ensure security and accuracy. In several countries, this system is not only used to enhance the efficiency of financial services but also to support efforts to prevent various forms of crime, including child sexual exploitation and human trafficking. One of the most significant examples of e-KYC implementation is in India with the use of the Aadhaar system, which is the largest biometric identification system in the world. Aadhaar, introduced in 2009, integrates biometric information such as fingerprints and iris scans into a centralized database maintained by the Indian government.²⁷ More than one billion Indian citizens are registered in this system, and Aadhaar

²⁷ Nair, Vijayanka. "An eye for an I: recording biometrics and reconsidering identity in postcolonial India." *Contemporary South Asia* 26.2 (2018): 143-156, <https://doi.org/10.1080/09584935.2017.1410102>.

has enabled financial institutions to quickly and accurately verify their customers' identities. This system has not only helped to increase financial inclusion by providing easier access to banking services for previously unbanked populations but has also combated various forms of fraud and financial crimes that often arise due to the misuse of false identities. The advantage of Aadhaar in terms of fast and efficient identity verification makes it effective in helping to prevent child sexual exploitation through illegal financial transactions. By ensuring that customer identities can be accurately verified, the system reduces the likelihood of criminals using fake identities to conduct transactions related to human trafficking or child exploitation. In this regard, Aadhaar can be an effective tool in supporting global efforts to combat complex transnational crimes such as child sexual exploitation. In India, Aadhaar gained legal legitimacy through a Supreme Court ruling in 2018 that deemed Aadhaar valid for specific purposes, such as government subsidies. However, more comprehensive data protection legislation, such as the Personal Data Protection Bill, is still under discussion. This law is expected to provide a clearer legal framework for protecting citizens' personal data, including the biometric data used in the e-KYC system.

In comparison, the European Union, through the General Data Protection Regulation (GDPR), adopts a much stricter approach when it comes to personal data protection, including biometric data used in the e-KYC process.²⁸ GDPR imposes rigorous requirements on financial institutions and other entities handling personal data, ensuring that customer privacy is upheld at all stages of data processing. Failure to comply with these strict regulations can result in hefty fines, potentially reaching up to 4% of a company's annual global turnover or €20 million, whichever is greater. The GDPR's approach to data protection emphasizes the principle of data minimization, which requires that only the necessary personal data be collected and processed, and that it be done transparently, with clear consent from the individuals involved. This is

²⁸ Hoofnagle, Chris Jay, et al. "The European Union general data protection regulation: what it is and what it means." *Information & Communications Technology Law* 28.1 (2019): 65-98, <https://doi.org/10.1080/13600834.2019.1573501>.

particularly relevant to the use of biometric data, such as fingerprints and facial recognition, in e-KYC systems. Under GDPR, biometric data is classified as sensitive data, which means that its processing is subject to even stricter conditions, requiring explicit consent and stronger safeguards to prevent misuse.

In the context of e-KYC in the European Union, the balance between privacy protection and effective crime prevention is crucial. While e-KYC systems are designed to streamline customer onboarding processes and monitor transactions in real-time, ensuring that financial institutions can detect suspicious activities such as money laundering or transactions related to child sexual exploitation, they must also rigorously protect the privacy rights of individuals. Financial institutions in Europe are required to implement robust security measures, including encryption, anonymization, and regular data audits, to prevent unauthorized access to sensitive customer information. Moreover, the GDPR grants individuals several key rights over their data, such as the right to be informed about how their data is used, the right to access their data, the right to correct any inaccuracies, and the right to have their data erased under certain conditions. This creates a legal environment where citizens have a higher degree of control over their personal information compared to other regions, such as India, where systems like Aadhaar may centralize vast amounts of personal data without offering the same level of individual control. Despite the stringent privacy requirements, the implementation of e-KYC in the EU is still highly effective in combating crimes like child sexual exploitation and human trafficking. Financial institutions leverage advanced technologies such as artificial intelligence (AI) and machine learning (ML) to identify suspicious transactions while adhering to GDPR's privacy standards. These systems use sophisticated algorithms to analyze patterns in financial data, detecting irregularities that could indicate illegal activities, all without compromising the security of personal data. For instance, many European countries have developed specific frameworks to monitor and report transactions that may be linked to human trafficking or child exploitation. These frameworks often rely on close collaboration between financial institutions, law enforcement agencies, and regulators to ensure that suspicious activity reports (SARs) are swiftly acted upon, while still maintaining full compliance with GDPR requirements. This

dual focus on data protection and crime prevention highlights the EU's commitment to safeguarding individual rights while effectively addressing complex transnational crimes.

In the United States, the implementation of e-KYC (electronic Know Your Customer) continues to evolve and has become a major focus for financial institutions in addressing various threats, including money laundering and terrorism financing.²⁹ The Financial Crimes Enforcement Network (FinCEN), as the regulatory authority, plays a key role in establishing guidelines to combat illegal financial activities. FinCEN requires financial institutions to strictly monitor suspicious transactions, including those potentially related to child sexual exploitation, in line with global efforts to stop illegal trade and human rights violations. Technology-driven transparency becomes a key strategy in revolutionizing rights supervision.³⁰ The adoption of e-KYC technologies, such as AI and biometrics, has been embraced by several large financial institutions, particularly to enhance security and efficiency in customer identification processes. These technologies enable automatic detection of transaction anomalies that may signal suspicious activities, allowing institutions to respond more swiftly. AI can process large volumes of data, detect unusual patterns, and conduct real-time risk assessments, accelerating the detection of financial activities linked to child sexual exploitation or other crimes.

The implementation of e-KYC introduces several significant challenges, particularly in the areas of data protection, technological reliability, and the readiness of financial institutions to adopt and adapt to these new technologies. Data protection emerges as a critical concern, given that e-KYC processes often involve the collection and storage of sensitive personal information, such as biometric data and transaction histories. Ensuring the security of this data against breaches and unauthorized access is paramount, especially as the consequences of misuse can be severe, both for individuals and institutions. Additionally, financial institutions must navigate the complexities of integrating

²⁹ Perlman, Leon, and Gurung, Nora. "Focus note: the use of eKYC for customer identity and verification and AML." *Available at SSRN 3370665* (2019).

³⁰ Widyawati, Anis, et al. "The Urgency of Supervision Institutions in Implementing Prisoners' Rights as an Effort to Restructure Criminal Execution Laws." *Jambura Law Review* 7.1 (2025): 127-151. <https://doi.org/10.33756/jlr.v7i1.27595>

advanced e-KYC technologies into their existing systems, which may require substantial investment in infrastructure and staff training.

On the technological front, tools such as artificial intelligence (AI) and biometric systems offer promising solutions to enhance the efficiency and accuracy of identity verification and financial crime prevention. AI, for instance, can analyze vast amounts of transaction data in real time, identifying patterns and anomalies that may indicate illicit activities, such as money laundering or child sexual exploitation. Similarly, biometric verification, through methods like facial recognition or fingerprint scanning, provides a robust mechanism to ensure that only authorized individuals can access financial services. However, these technologies are not without their limitations. Facial recognition systems, for example, have been shown to perform less effectively for individuals with certain physical characteristics, such as darker skin tones or unique facial structures, which can lead to errors in identity verification and potential exclusion.

Despite these challenges, the opportunities presented by e-KYC technologies are substantial. When implemented correctly, e-KYC can significantly enhance the security of financial transactions, making it more difficult for perpetrators of crimes, including child sexual exploitation, to exploit financial systems. AI's capacity to detect suspicious transaction patterns, combined with the precision of biometric systems, offers a dual-layered defense against unauthorized access and fraudulent activities. These advancements enable financial institutions to act swiftly in identifying and addressing risks, strengthening their overall resilience against criminal exploitation.

Moreover, the proper integration of e-KYC not only bolsters financial security but also aligns with global regulatory frameworks, which increasingly emphasize the need for robust measures to prevent financial crimes. Financial institutions that effectively leverage e-KYC can ensure compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) standards while building trust among their customers. By addressing the challenges and maximizing the potential of these technologies, e-KYC has the capacity to transform financial systems into more secure, transparent, and consumer-friendly environments.

Conclusion

The Know Your Customer (KYC) model is a crucial strategic framework in preventing the misuse of financial services, particularly in transactions related to child sexual exploitation. In the digital and globalized era, child sexual exploitation often exploits gaps in the financial system, including anonymous transactions that are difficult to trace. By integrating rigorous processes of identification, verification, and continuous monitoring of financial transactions, KYC plays a key role in detecting suspicious activities, including those related to child exploitation. The use of advanced technologies like biometrics and artificial intelligence (AI) within the e-KYC model allows financial institutions to verify customer identities more quickly and accurately, as well as to monitor unusual transaction patterns. This becomes essential in preventing the exploitation of financial systems by child sexual exploitation perpetrators, who often attempt to hide illegal activities through subtle or unconventional transaction behaviors. From a legal perspective, the implementation of KYC must be supported by a robust legal framework that encompasses anti-money laundering (AML), counter-terrorist financing (CTF), and human rights protection, especially in terms of children's rights. The Convention on the Rights of the Child (CRC) mandates that states protect children from all forms of exploitation, including financial channels. Strengthening KYC implementation requires legal reforms that expand its coverage to digital transactions and cryptocurrencies, as well as improving law enforcement's ability to monitor suspicious activities. For instance, there is a need for greater harmonization of regulations across countries, as child sexual exploitation often involves transnational networks. Moreover, e-KYC technologies provide innovative solutions for mitigating financial risks through the use of biometric identification and AI. However, the adoption of these technologies also introduces challenges in terms of data privacy and system accuracy. Therefore, regulations must ensure the protection of personal data and clearly define the legal liabilities of financial institutions that fail to meet KYC standards. In countries like India and the European Union, the implementation of e-KYC has proven effective in combating financial crimes, but it is also balanced by strict data protection standards. In

conclusion, the implementation of a strong KYC model, integrated with cutting-edge technologies and supported by a comprehensive legal framework, can significantly contribute to preventing the misuse of financial services for child sexual exploitation. Financial institutions must take proactive steps to implement KYC and e-KYC effectively, while also collaborating with law enforcement to ensure that suspicious transactions are swiftly identified and acted upon. This comprehensive approach not only aids in combating child exploitation but also ensures compliance with global regulations, thereby safeguarding the overall integrity of the financial system.

References

- Josenhans, Valentine, et al. "Gender, rights and responsibilities: The need for a global analysis of the sexual exploitation of boys." *Child Abuse & Neglect* 110 (2020): 1–7, <https://doi.org/https://doi.org/10.1016/j.chiabu.2019.104291>.
- Jonathan, Okpuvwie Ejuvweyere, et al. "Impacts of crime on socio-economic development." *Mediterranean Journal of Social Sciences* 12.5 (September 5, 2021): 71–81, <https://doi.org/10.36941/mjss-2021-0045>.
- Simon, June, Ann Luetzow, and Jon R. Conte. "Thirty years of the convention on the rights of the child: Developments in child sexual abuse and exploitation." *Child abuse & neglect* 110 (2020): 1–5, <https://doi.org/https://doi.org/10.1016/j.chiabu.2020.104399>.
- Pendergast, Kirra. "Protecting Children Online: Strategies for a Safer Future." *Ubiquity Proceedings* 3.1 (June, 2023): 334–39, <https://doi.org/10.5334/uproc.105>.
- Stamatakis, Caroline E., et al. "Sexual violence prevalence and related pregnancy among girls and young women: a multicountry analysis." *Journal of interpersonal violence* 37.3-4 (2022): NP2428–NP2441, <https://doi.org/10.1177/0886260520936366>.
- Barbara, Giusy, et al. "Sexual violence against adolescent girls: labeling it to avoid normalization." *Journal of Women's Health* 26.11 (2017): 1146–1149, <https://doi.org/10.1089/JWH.2016.6161>.

- Anubhab Mukherjee, "Silent Suffering: The Unspoken Reality of Male," *International Journal of Research and Review* 11, no. August (2024): 613–24, <https://doi.org/https://doi.org/10.52403/ijrr.20240866>.
- Adrial Akbar, "PPATK Temukan Transaksi Rp 114 M Terkait Pornografi Anak Selama 2022," *detikNews*, 2022, <https://news.detik.com/berita/d-6485840/ppatk-temukan-transaksi-rp-114-m-terkait-pornografi-anak-selama-2022>.
- Cubitt, Timothy IC, et al. "Understanding the offline criminal behavior of individuals who live stream child sexual abuse." *Journal of interpersonal violence* 38.9-10 (2023): 6624-6649, <https://doi.org/10.1177/08862605221137712>.
- Jain, Harsh, et al. "Financial investment recommendation and decentralized account management." *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, (2020): 1–6, <https://doi.org/10.1109/ICCCNT49239.2020.9225326>.
- Fernando, Zico Junius, et al. "The Role of Neuroprediction and Artificial Intelligence in the Future of Criminal Procedure Support Science: A New Era in Neuroscience and Criminal Justice." *Yuridika* 38.3 (2023): 593-620, <https://doi.org/10.20473/ydk.v38i3.46104>.
- Widyawati, Anis, et al. "Urgency of the Legal Structure Reformation for Law in Execution of Criminal Sanctions." *Lex Scientia Law Review* 6.2 (2022): 327-358, <https://doi.org/10.15294/lesrev.v6i2.58131>.
- Nilsson, Johan. "Know your customer: Client captivation and the epistemics of market research." *Marketing Theory* 19.2 (2019): 149-168, <https://doi.org/10.1177/1470593118787577>.
- Krist, By Marcel. "Will Financial Institutions Ever Achieve a 100% Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Rules?." *The RegTech Book* (2019), <https://doi.org/10.1002/9781119362197.CH30>.
- See, Benedictus Renny, and Ahmadi Miru. "Know Your Customer (KYC) Principles Relates to Bank Confidentiality as an Effort to Prevent Money Laundering Crimes." *JL Pol'y & Globalization* 81 (2019): 101, <https://doi.org/10.7176/JLPG>.

- Hasanli, Zamina "FATF Recommendations as A Major Tool for AML," *Scientific Research International Online Scientific Journal* 3, no. 4 (2023): 1–23, <https://doi.org/10.36719/2789-6919/20/91-93>.
- Verma, Kavery, et al. "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking." *2023 9th International Conference on Signal Processing and Communication (ICSC)*. IEEE (2023): 319–24, <https://doi.org/10.1109/ICSC60394.2023.10441596>.
- Lawton, George. "Biometrics: a new era in security." *Computer* 31.08 (1998): 16-18, <https://doi.org/10.1109/MC.1998.707612>.
- Sharma, Preeti, A. Shanker Prakash, and Anjul Malhotra. "Application of Advanced AI Algorithms for Fintech Crime Detection." *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, (2024): 1-6 , <https://doi.org/10.1109/ICCCNT61001.2024.10725857>.
- Kingdon, Jason. "AI fights money laundering." *IEEE Intelligent Systems* 19.3 (2004): 87-89, <https://doi.org/10.1109/MIS.2004.1>.
- Legg, Philip A., et al. "Automated insider threat detection system using user and role-based profile assessment." *IEEE Systems Journal* 11.2 (2015): 503-512., <https://doi.org/10.1109/JSYST.2015.2438442>.
- Alahira, Joshua, et al. "The role of artificial intelligence in enhancing tax compliance and financial regulation." *Finance & Accounting Research Journal* 10 (2024): 241–251, <https://doi.org/10.51594/FARJ.V6I2.822>.
- Perlman, Leon, and Nora Gurung. "Focus note: the use of eKYC for customer identity and verification and AML." *Available at SSRN* 3370665 (2019): 1–28, <https://doi.org/10.2139/SSRN.3370665>.
- Verma, Kavery, et al. "Efficient e-KYC Authentication System: Redefining Customer Verification in Digital Banking." *2023 9th International Conference on Signal Processing and Communication (ICSC)*. IEEE, 2023.
- Chakraborty, S., et al. "E-KYC system using blockchain." *International Journal for Research in Applied Science and Engineering Technology* 11.7 (2023): 1174-1181, <https://doi.org/10.22214/ijraset.2023.54834>.
- Nair, Vijayanka. "An eye for an I: recording biometrics and reconsidering identity in postcolonial India." *Contemporary South Asia* 26.2

(2018): 143-156,
<https://doi.org/10.1080/09584935.2017.1410102>.

Hoofnagle, Chris Jay, et al. "The European Union general data protection regulation: what it is and what it means." *Information & Communications Technology Law* 28.1 (2019): 65-98, <https://doi.org/10.1080/13600834.2019.1573501>.

Perlman, Leon, and Gurung, Nora. "Focus note: the use of eKYC for customer identity and verification and AML." *Available at SSRN 3370665* (2019).

Widyawati, Anis, et al. "The Urgency of Supervision Institutions in Implementing Prisoners' Rights as an Effort to Restructure Criminal Execution Laws." *Jambura Law Review* 7.1 (2025): 127-151. <https://doi.org/10.33756/jlr.v7i1.27595>

*Justitiae non est neganda,
non differenda*

Acknowledgment

We sincerely express our deep gratitude to all individuals and organizations whose invaluable support and contributions have greatly influenced the completion of this article. We are also profoundly thankful to the authors of books, journal articles, and other academic resources that have provided essential insights and a solid foundation for our analysis. Recognizing that academic work is an ongoing process of refinement, we warmly invite readers to offer their feedback and constructive criticism. This openness reflects our commitment to continually improving the quality and relevance of our research. We wholeheartedly hope that this article serves as a valuable resource for academics, practitioners, and the broader community in understanding and addressing complex legal challenges in everyday life.

Funding Information

None

Conflicting Interest Statement

There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

In an effort to ensure the academic integrity and authenticity of published works, we are firmly committed to the principles of publishing ethics and material authenticity. Every work we publish undergoes a rigorous process of authenticity checking to prevent plagiarism and ensure that all sources are properly acknowledged, as well as adhering to applicable standards of research ethics. We emphasize that each author is responsible for providing work that is not only innovative and contributes to existing knowledge but also upholds academic integrity. Violations of these principles will be taken seriously, and necessary steps will be taken to correct any errors or discrepancies. With this, we are committed to promoting an ethical and responsible academic environment where the originality and integrity of the work are placed at the highest level.