HSR London International Conference on Multidisciplinary Academic Research
(HSR-ICMAR) 2026
https://houghtonstreetreview.com/index.php/conference

AML AND KYC OBLIGATIONS AND PERSONAL DATA PROTECTION IN PAYMENT SYSTEMS: A COMPARATIVE STUDY OF INDIA AND UZBEKISTAN

Shashank Sidharth
National Forensic Sciences University Gandhinagar, India &
Tashkent State University of Law, Uzbekistan

Dr Anna Ubaydullaev
Under the Supervision of
https://doi.org/10.5281/zenodo.21336802

Abstract

The rapid expansion of digital payment systems in India and Uzbekistan has transformed financial transactions while simultaneously amplifying risks of money laundering, terrorist financing, identity theft, and online financial fraud. In response, both jurisdictions have strengthened Anti-Money Laundering (AML) and Know Your Customer (KYC) frameworks, mandating extensive collection, verification, monitoring, and retention of customer data by banks and payment service providers. At the same time, emerging data protection regimes particularly India's Digital Personal Data Protection Act, 2023, and Uzbekistan's Law "On Personal Data" seek to safeguard informational privacy through principles such as legality, purpose limitation, data minimisation, storage limitation, accountability, and security safeguards. This thesis conducts a comparative analysis of the legal and regulatory frameworks governing AML/KYC obligations and personal data protection in digital payment systems in India and Uzbekistan, examining statutory provisions, regulatory directions, and policy reforms. It evaluates the extent to which each jurisdiction reconciles financial integrity objectives with the right to privacy and protection of personal data, focusing on issues such as customer due diligence, continuous transaction monitoring, data retention, data localisation, cross- border data transfers, and cybersecurity obligations. The study argues that while both countries have significantly modernised their legal frameworks and aligned them with international standards, they have not yet achieved an optimal balance between AML enforcement and privacy protection. It concludes by proposing a set of reforms including clearer rules on data retention and deletion, limits on excessive data collection, regulation of automated profiling, enhanced transparency obligations, and promotion of privacy- by- design—to ensure that efforts to combat financial crime do not unduly compromise fundamental rights in the digital payment ecosystem.

Keywords: Anti-Money Laundering (AML), Know Your Customer (KYC) ,Digital payment systems, Personal data protection, Data localisation, India, Uzbekistan

The rapid growth of digital payment systems has changed the way people and businesses transfer money across the world. Over the last decade, both India and Uzbekistan have experienced a significant shift from cash-based transactions to digital payment methods. Mobile banking, QR code payments, internet banking, digital wallets and instant payment systems have become an essential part of everyday life. Governments in both countries have actively promoted digital payments because they improve financial inclusion, reduce dependence on cash, increase transparency, and help bring more people into the formal financial system. At the same time, the rise of digital payments has also increased the risks of money laundering, terrorist financing, identity theft and online financial fraud. To address these challenges, regulators have strengthened Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements for banks and payment service providers.

AML and KYC obligations require financial institutions to verify the identity of customers before allowing them to use financial services. These measures help prevent criminals from using banks or payment platforms to hide illegally obtained money or finance unlawful activities. However, compliance with AML and KYC laws also requires payment service providers to collect, process and store large amounts of personal information. Identity documents, addresses, mobile numbers, biometric information, photographs, bank account details, transaction history and even behavioural patterns may be collected during this process. As a result, an important legal question arises: how can governments effectively prevent financial crime without unnecessarily interfering with an individual's right to privacy and protection of personal data?

Both countries have rapidly expanding digital payment ecosystems and have introduced modern legal frameworks to regulate payment systems, prevent money laundering and protect personal data. Although their legal systems differ, both jurisdictions face similar challenges in balancing financial security with individual privacy. The study therefore seeks to analyse whether the existing legal frameworks achieve this balance and what reforms may be necessary.

In India, digital payments have grown rapidly due to technological innovation and government initiatives such as Digital India and the introduction of the Unified Payments Interface (UPI). Today, millions of people use platforms such as PhonePe, Google Pay, Paytm and BHIM for daily transactions. A vegetable vendor, taxi driver or small shopkeeper can receive payments instantly through a QR code without using cash. While this convenience has transformed commerce, it has also created opportunities for cybercriminals to misuse digital payment channels for fraud and money laundering. Consequently, India has strengthened its AML framework through the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money Laundering (Maintenance of Records) Rules and the Reserve Bank of India's Master Directions on KYC. These laws require banks, payment banks, prepaid payment instrument issuers and other regulated entities to verify customer identity, monitor transactions, maintain records and report suspicious transactions to the Financial Intelligence Unit-India (FIU-IND).

Alongside financial regulation, India has also introduced the Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes a legal framework governing the collection and processing of digital personal data. The Act recognises that individuals have a legitimate interest in controlling how their personal information is collected and used. It introduces principles such as lawful processing, accountability, security safeguards and protection against misuse of personal data. Payment service providers must therefore comply not only with AML obligations but also with the requirements of the DPDP Act and sector-specific RBI regulations relating to payment data storage, cybersecurity and data localisation.

Uzbekistan has similarly modernised its financial sector through extensive legal reforms. The Law "On Payments and Payment Systems" regulates payment organisations, electronic money institutions and payment infrastructure. The Central Bank of Uzbekistan supervises payment service providers and ensures compliance with AML and Counter Financing of Terrorism (CFT) obligations. Personal data is protected under the Law "On Personal Data", supported by regulations governing the processing, storage and transfer of personal information. Initially, Uzbekistan adopted strict data localisation requirements requiring personal data of Uzbek citizens to be stored within the country. However, recent legal reforms have gradually relaxed these restrictions to facilitate international business, attract foreign investment and encourage the entry of global payment platforms into the Uzbek market.

Although the legal frameworks of India and Uzbekistan differ in structure, they pursue similar policy objectives. Both countries seek to create secure payment systems that promote economic development while protecting users from financial crime. At the same time, both recognise that excessive collection or misuse of personal data may undermine public trust in digital financial services.

AML obligations are primarily intended to prevent criminals from disguising the origin of illegally obtained money. Money laundering generally involves placing illegal funds into the financial system, moving them through multiple transactions to conceal their origin, and finally integrating them into the legitimate economy. Without proper customer verification, criminals can easily exploit payment systems using false identities or anonymous accounts.

For this reason, KYC has become the first line of defence against financial crime. Before opening an account or providing payment services, financial institutions must verify the customer's identity using reliable documents. In India, Aadhaar, PAN cards, passports and voter identity cards are commonly used for this purpose. RBI has also introduced Video Customer Identification Process (V-CIP), allowing customers to complete KYC remotely through secure video verification. Similarly, payment organisations in Uzbekistan require customers to submit official identification documents before accessing certain financial services.

For example, if a person wishes to open a digital wallet in India and transfer large amounts of money every day, the payment company must verify the person's identity before permitting such transactions. Likewise, if an individual in Uzbekistan opens multiple electronic payment accounts under different names to transfer suspicious funds, AML monitoring systems are expected to identify unusual activity and report it to the competent authorities.

Modern AML compliance no longer ends with customer identification. Financial institutions continuously monitor customer behaviour throughout the business relationship. Sophisticated software analyses transaction patterns to detect suspicious activities such as unusually large transfers, repeated cross-border payments, structuring of transactions below reporting thresholds or rapid movement of funds through multiple accounts. Artificial intelligence and machine learning increasingly assist banks in identifying suspicious financial behaviour.

Although these technologies improve financial security, they also create privacy concerns. Continuous monitoring means that payment service providers possess detailed information about an individual's spending habits, travel patterns, business activities and financial preferences. For example, regular payments to hospitals may indirectly reveal medical conditions, while donations to certain organisations may indicate political or religious beliefs. Such information deserves strong legal protection because it relates to an individual's private life.

This is where personal data protection laws become particularly important. Both India and Uzbekistan recognise that personal information should not be collected or processed without legal justification. Data protection laws are based upon several important principles, including legality, purpose limitation, data minimisation, storage limitation, accountability and security.

The principle of legality requires that personal data must be processed under a valid legal basis. In the context of AML compliance, payment institutions generally process customer information because the law requires them to do so. Therefore, unlike marketing activities, AML processing usually does not depend upon customer consent. Nevertheless, payment institutions remain responsible for ensuring that the collected information is used only for lawful purposes.

The principle of purpose limitation requires organisations to use personal information only for the purpose for which it was originally collected. Information collected during KYC verification should ordinarily be used for regulatory compliance and prevention of financial crime. However, concerns arise when companies subsequently use the same information for advertising, customer profiling or commercial marketing without adequate legal justification. For example, if a payment application collects identity documents for KYC purposes but later analyses customer spending habits to sell insurance or investment products, questions may arise regarding compliance with data protection principles.

Another important principle is data minimisation. Financial institutions should collect only the information necessary to satisfy legal requirements. However, in practice many organisations adopt a

cautious approach by requesting more information than may actually be required. This phenomenon is often called defensive compliance. Banks may collect additional documents simply to avoid regulatory criticism, even when the additional information has little practical value in assessing money laundering risks. Such practices increase compliance costs and unnecessarily expose customers to greater privacy risks.

Data retention represents another significant challenge. AML laws generally require financial institutions to preserve customer records and transaction information for several years after the end of a business relationship. These records are important because financial investigations may begin long after suspicious transactions have occurred. However, prolonged retention also increases the risk of unauthorised access, cyberattacks and misuse of personal information. Data protection laws generally encourage organisations to delete personal information once it is no longer necessary, creating an apparent tension between AML obligations and privacy principles.

Data localisation has become another major area of regulatory debate. India has adopted relatively strict payment data localisation requirements through RBI directions requiring payment system data to be stored within India. The objective is to strengthen regulatory oversight, improve law enforcement access and ensure national control over critical financial infrastructure. For example, if payment transaction data is stored exclusively on foreign servers, Indian regulatory authorities may face practical difficulties in obtaining timely access during criminal investigations.

Uzbekistan initially followed a similar approach by requiring personal data relating to its citizens to be stored on domestic servers. However, recognising the importance of international business and fintech investment, recent reforms have introduced greater flexibility regarding cross-border data transfers. This reflects the country's broader objective of integrating with the global digital economy while maintaining adequate safeguards for personal information.

Cross-border data transfers have become increasingly common because many payment systems operate through international networks. International card payments, online shopping platforms and multinational payment gateways frequently require customer information to move across different jurisdictions. While such transfers improve efficiency, they also raise concerns regarding differences in privacy standards between countries. Strong legal safeguards are therefore necessary to ensure that personal information remains protected regardless of where it is processed.

Cybersecurity is closely connected with personal data protection. Digital payment platforms store enormous quantities of sensitive financial information, making them attractive targets for hackers. A successful cyberattack may expose identity documents, bank account details, payment histories and authentication credentials belonging to millions of customers. Consequently, both India and Uzbekistan require payment service providers to implement robust cybersecurity measures including encryption, secure authentication, access controls, regular security audits and incident reporting mechanisms. Protecting personal data is therefore not merely a legal obligation but also an essential component of maintaining trust in digital payment systems.

International organisations have also recognised the need to balance AML compliance with privacy rights. The Financial Action Task Force (FATF), whose recommendations influence AML legislation across the world, encourages countries to adopt risk-based AML frameworks while respecting fundamental rights and ensuring appropriate protection of personal information. Similarly, the Financial Stability Board and other international institutions increasingly emphasise that effective financial regulation and responsible data governance should complement rather than contradict each other.

The comparative analysis demonstrates that India possesses a relatively mature regulatory framework owing to its highly developed digital payment ecosystem. The RBI has issued extensive operational guidelines covering KYC, cybersecurity, payment data storage and digital payment security. The enactment of the DPDP Act further strengthens India's legal framework by establishing

comprehensive obligations regarding personal data processing. Nevertheless, greater regulatory clarity is still required regarding the interaction between AML obligations and data protection principles, particularly concerning data retention, automated decision-making and secondary use of customer information.

Uzbekistan has also made remarkable progress in modernising its financial and data protection laws. Legal reforms have significantly improved payment regulation while gradually aligning domestic legislation with international standards. However, further harmonisation between AML obligations and personal data protection remains necessary, particularly regarding data retention periods, cross-border transfers and supervisory coordination.

Conclusion

The comparative study of India and Uzbekistan demonstrates that AML and KYC frameworks have become central pillars of the regulatory architecture governing digital payment systems in both jurisdictions. By mandating robust customer identification, ongoing due diligence, and detailed record-keeping, these regimes seek to prevent the misuse of financial channels for money laundering, terrorist financing, and related offences. However, the very mechanisms that enhance financial integrity extensive data collection, continuous monitoring, and prolonged retention of customer information create significant risks for personal privacy and data protection.

India's legal framework reflects a relatively advanced and integrated approach, combining the Prevention of Money Laundering Act, 2002, its accompanying rules, and the Reserve Bank of India's Master Directions on KYC with the Digital Personal Data Protection Act, 2023. This structure provides detailed operational guidance for regulated entities and establishes general obligations on lawful processing, purpose limitation, accountability, and security in relation to digital personal data. Yet, important gaps remain, particularly regarding the reconciliation of AML-driven retention requirements with storage limitation principles, the permissible scope of secondary use of customer information, and the governance of automated risk-scoring and profiling in AML compliance systems.

Uzbekistan, though at a different stage of financial sector development, has undertaken substantial reforms through the Law "On Payments and Payment Systems" and the Law "On Personal Data," complemented by regulatory measures of the Central Bank and sectoral authorities. These measures have enhanced supervision of payment organisations, clarified AML/CFT obligations, and progressively relaxed earlier data localisation mandates to facilitate cross-border services and foreign investment. Nonetheless, challenges persist in aligning AML data retention rules with data protection principles, ensuring consistent standards for cross-border data transfers, and strengthening institutional coordination between AML and data protection regulators.

A key finding of this thesis is that AML and personal data protection should not be treated as inherently conflicting objectives but as complementary components of a resilient digital financial ecosystem. Effective AML frameworks depend on public trust in the secure and responsible handling of personal information, while credible data protection regimes must accommodate legitimate law-enforcement and regulatory needs. To move towards a more balanced model, both India and Uzbekistan should adopt a risk-based approach that narrows the scope of mandatory data collection to what is strictly necessary, introduces differentiated retention periods aligned with risk levels, and mandates periodic review and deletion of data that is no longer required for regulatory or investigative purposes.

Further, regulators should issue clear guidance on the permissible use of customer data collected for AML/KYC purposes, expressly limiting its deployment for unrelated commercial activities such as targeted marketing or non-essential profiling. Specific safeguards should address the growing reliance on artificial intelligence and machine learning in transaction monitoring, including transparency obligations, auditability, and mechanisms for human oversight of automated decisions. Strengthened cybersecurity obligations, regular security audits, and mandatory breach notification requirements are

essential to protect the vast repositories of sensitive financial and identity data held by payment service providers. By implementing these reforms, India and Uzbekistan can enhance confidence in digital payment systems, support responsible innovation, and ensure that the fight against financial crime proceeds in harmony with the protection of fundamental rights to privacy and personal data.

Bibliography

1. Prevention of Money Laundering Act, No. 15 of 2003, INDIA CODE (2003).
2. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
3. Law of the Republic of Uzbekistan on Payments and Payment Systems, No. ZRU-573 (2019) (Uzb.).
4. Law of the Republic of Uzbekistan on Personal Data, No. ZRU-547 (2019) (Uzb.).
5. Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (India).
6. Reserve Bank of India, Master Direction – Know Your Customer (KYC) Direction, 2016 (as amended).
7. Reserve Bank of India, Circular on Storage of Payment System Data (Apr. 6, 2018).
8. Central Bank of the Republic of Uzbekistan, Regulation on Requirements for the Internal Control System to Counteract Legalization of Criminal Proceeds and Financing of Terrorism (AML/CFT Regulation) (Uzb.).
9. Government of India, Ministry of Electronics & Information Technology, Digital India Programme (2015).