WASHED IN PLAIN SIGHT: THE LEGAL AND POLICY BLIND SPOT IN PAYMENT GATEWAY LAUNDERING

Vridhi Suri, Symbiosis Law School, Pune

ABSTRACT

The growth and expansion of India's fintech ecosystem has brought with it a parallel rise in novel forms of financial crime. One such threat that is now seeing the light of the day is payment gateway laundering, which in layman terms is the misuse of legitimate digital payment intermediaries to disguise and process illicit funds. This paper explores how shell entities, fake merchants, and deceptive invoices are used to route illegal proceeds from activities such as online gambling, crypto scams, and fraud through regulated payment gateways, masking them to appear as ordinary commercial transactions.

Unlike traditional modes of money laundering, this form exploits the legal and technological trust infrastructure of licensed payment service providers. The process is often concealed behind layers of business activity that appear legitimate prime facie, making it difficult not only to detect, but also to prosecute. The paper maps the typology of such laundering, examines the roles of intermediaries like payment aggregators, banks, and front-end merchants, and evaluates the regulatory and legal framework governing these transactions in India.

By focusing on the ambiguities in current law, including the Information Technology Act, 2000 [1]and the Prevention of Money Laundering Act[2], the study highlights the challenges law enforcement and regulators face in identifying and attributing liability for such crimes. The phenomenon of payment gateway laundering reflects a broader concern about the evolving nature of white collar crime in the digital economy.

[1] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[2] The Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament (India)

Introduction

"In the age of digital convenience, crime no longer lurks in the shadows, it integrates itself into the system." What was once the domain of shell companies and offshore accounts is now subtly woven into the infrastructure of fintech. As payment gateways become the arteries of modern commerce, they also risk becoming conduits for laundering illicit funds, *washed in plain sight*, under the guise of legitimate business.

The fast paced growth of the fintech infrastructure in India has revolutionized the way financial transactions take place. From Unified Payments Interface (UPI) to digital wallets and online payment aggregators, the Indian consumer and business landscape has undergone a significant transformation. At the heart of this revolution lie payment gateways, which are simply platforms that facilitate real-time transactions between customers, merchants, and banks. However, alongside the convenience and efficiency offered by these platforms, a new and under-examined form of financial misconduct has emerged: namely, payment gateway laundering.

Payment gateway laundering can simply be summarises as the use of legitimate digital payment processors to disguise or route illegal or deceptive transactions. Akin to traditional money laundering, which conceals the illicit origin of funds, payment gateway laundering involves the strategic use of technology to make illegitimate funds appear legitimate. This is often facilitated through fake merchants, shell companies, manipulated invoices, or layering techniques where multiple merchant identities are used to route illicit earnings through genuine platforms. The result is a fraudulent, criminal, or unauthorized transactions which is portrayed as "clean" and processed as though they were legitimate business dealings.

The fintech boom has inadvertently laid a fertile foundation for such laundering techniques. The ease of merchant onboarding, the automation of payment processes, and the digital disintermediation of financial services have significantly reduced friction in the system. But in doing so, the traditional gatekeeping functions such as due diligence, KYC (Know Your Customer), and audit trails have also been diluted, or neglected. Small merchants, especially in sectors such as gaming, ed-tech, gambling, or crypto, can now create multiple payment fronts or utilise shell companies to push large sums of money through seemingly legal channels. This creates a structural vulnerability that is being increasingly exploited for white collar crimes, which refers to crimes that are non-violent but involve deceit, fraud, and abuse of trust for

financial gain.

This paper seeks to address the following critical research questions:

1. Can payment gateways be misused for white collar crimes, and if so, what forms does this misuse take?

2. Who bears legal and regulatory liability in cases of payment gateway laundering, is it the merchant, the payment processor, or the bank?

3. Is Indian law currently equipped to recognize, regulate, and prosecute this form of digital financial crime, or are there significant gaps in the legal framework?

Understanding payment gateway laundering through the lens of white collar crime becomes crucial, as it exhibits all the classic characteristics of the same: abuse of position and infrastructure, intent to deceive, concealment of financial wrongdoing, and cross-border manipulation of regulatory gaps. While posing a significant threat to the financial infrastructure of a country, this form of crime often goes unnoticed in public discourse and law enforcement due to the complex technological layers that obscure accountability of the same. It is time to reclassify and recognize such activity not merely as a compliance failure or regulatory lapse, but as criminal economic conduct with serious implications for the integrity of India's digital financial system.

By situating payment gateway laundering within the broader framework of white collar crime, this paper aims to highlight the urgent need for regulatory reform, criminal liability, and a more nuanced understanding of digital financial misconduct in the subcontinent.

How Does Payment Gateway Laundering Works?

Payment gateway laundering is a nuanced form of financial deception wherein criminal actors exploit legitimate digital payment infrastructure to conceal the true nature of illicit transactions. It closely mirrors traditional money laundering processes but is adapted to the high-speed, digital environment of modern fintech systems. The orchestrators of this scheme often involve the use of shell entities, fraudulent merchant accounts, and false commercial activity to obscure the origin and destination of illegal funds.

The typology of the fraud typically begins with the creation of a shell merchant, which is a company that exists only on paper or online, with no genuine business activity or physicality. This merchant may list itself as operating in a benign or low-risk sector, such as consultancy, digital marketing, or retail. Once the fake entity is created, it registers with a payment gateway such as Razorpay[3], PayU, or Stripe, all of which are designed to onboard small and medium merchants with minimal delay. These platforms generally require standard KYC documentation and bank details, but due to the sheer volume of applications and the lack of thorough background checks, fraudulent actors often slip through the cracks, and benefit from the same.

Upon registration, the shell merchant use the gateway to route illegal funds[4]. These funds may originate from a range of unlawful activities, including but not limited to online gambling rings, fraudulent loan apps, Ponzi schemes, crypto scams, adult content sales, or even narcotics transactions. The criminal entity generates fake invoices or uses bots to simulate customer activity, creating the illusion of legitimate business revenue. Payment gateways process these transactions like any other e-commerce operation, by deducting their service fee and transferring the remaining funds into the merchant's linked bank account. As a result, dirty money enters the system and exits as clean, "business" income, often with minimal oversight and scrutiny from regulators or enforcement bodies.

More advanced schemes involve layering, which is a method by which multiple shell or front merchants are used to further obscure the transaction trail. A single payment gateway may service dozens of such fronts, all of which are controlled by the same criminal network but listed under different names, industries, and locations. In some cases, "front" merchants are legitimate businesses who agree to route funds on behalf of third parties for a commission, thereby offering criminals a proxy shield.

Several real-world examples illustrate how this works. Fake e-commerce platforms have been created to sell non-existent products, where transactions are generated solely to launder money. In another case, adult content services were falsely registered as digital consultancy firms. Crypto gambling operations have also been disguised as IT service providers, with payment

[3] What is a Payment Gateway? How it Works with Example, https://razorpay.com/blog/payment-gateway-101/ (last visited Aug 4, 2025)
[4] Fintech: A Gateway to White Collar Crime, or to Financial Inclusion Aided by a Robust Regulatory Regime Lexology, https://www.lexology.com/library/detail.aspx?g=c1f28dcd-2f23-4026-b553-81ad54dadabf (last visited Aug 4, 2025)

links directing users to "training platforms" that are in fact betting portals. The recent investigations by Indian agencies into loan app frauds have revealed that Chinese-controlled apps routed hundreds of crores through payment gateways using fake merchant IDs.

The success of such laundering schemes lies in their digital opacity and the systemic assumption of legitimacy surrounding fintech platforms. Without stronger gatekeeping, these gateways become not just conduits of innovation, but also vehicles for financial crime.

Cases and Red Flags

While payment gateway laundering remains a relatively obscure concept in mainstream legal discourse, a growing number of real-world cases in India have exposed how digital payment systems are being systematically exploited to mask illicit transactions. These cases not only highlight the evolving tactics of financial criminals but also expose the vulnerabilities within India's fintech regulatory framework.

A prominent example came to light in 2022, when the Enforcement Directorate (ED) conducted raids on several fintech companies allegedly linked to Chinese-controlled loan apps[5]. These apps were offering small-ticket, high-interest loans to Indian consumers. They were found to have routed over ₹1,000 crore through Indian payment gateways like Razorpay and Cashfree. Investigations revealed that these entities had created fake merchant profiles, some posing as digital marketing firms or IT service providers, and used them to process large volumes of money, which was subsequently withdrawn into shell company bank accounts or routed offshore. In many instances, the entities disappeared after receiving the funds, leaving behind unpaid borrowers and fraudulent trails.

Another major instance of gateway laundering involved the illegal online gambling industry, where websites hosted abroad collected payments from Indian users using domestic payment gateways[6]. These gambling platforms disguised themselves as online training services or fantasy gaming platforms, thereby skirting Indian laws prohibiting online betting. The

[5] ED raid on loan apps reveals strong Chinese presence in crypto crimes Frontline, https://frontline.thehindu.com/columns/loan-apps-in-crypto-crimes/article65780036.ece (last visited Aug 4, 2025)

[6] *Home ministry warns against illegal digital payment gateways used by cybercriminals*, The Times of India, Oct. 28, 2024, https://timesofindia.indiatimes.com/india/home-ministry-warns-against-illegal-digital-payment-gateways/articleshow/114698595.cms (last visited Aug 4, 2025)

gateways, in turn, processed these transactions under mislabelled merchant categories, either due to lax due diligence or deliberate oversight.

Such cases expose a range of red flags that indicate possible laundering activity through payment gateways, instances of which include :

- Unusual Merchant Categories: Shell companies often list themselves under low-risk sectors such as "consulting" or "digital services" to avoid regulatory scrutiny.
- High Transaction Velocity with Low Value: Merchants processing hundreds of small transactions per day, usually under ₹2,000, which is masked as illicit activity.
- Excessive Refunds or Chargebacks: A high refund ratio, particularly within a short timeframe, may suggest false transactions or indicate bot generated payments.
- Common IPs Across Merchants: Technical analysis has revealed multiple merchant accounts created from the same IP address or device, indicating coordinated fraud networks.
- Short Lifespan of Merchant Accounts: Entities operating for only a few months before being deactivated or abandoned often suggest use for a specific laundering scheme.
- Mismatch in Business Description vs. Activity: A company listed as an “educational consultancy” with large daily inbound transactions and no visible marketing presence raises red flags.

Moreover, many shell merchants tend to share the same set of directors, addresses, or bank accounts, often through slightly modified names or IDs. These overlaps, though subtle, indicate the presence of a larger laundering network operating behind multiple fronts.

Despite these warning signs, enforcement often lags because payment gateways are treated as passive intermediaries, not active participants. Regulatory compliance is usually viewed through a civil or administrative lens, particularly focusing on KYC lapses, rather than through criminal frameworks addressing conspiracy, fraud, or abetment.

These real cases highlight the urgent need for a proactive, intelligence driven approach to monitor and intercept laundering through payment infrastructure. Ignoring these red flagged

risks paves way to a parallel financial system that undermines trust in India's digital economy.

Current Legal & Regulatory Framework in India

India's supervisory regime for digital payments has evolved rapidly to keep pace with the rapidly revolutionising fintech sector. However, when it comes to payment gateway laundering, the legal framework remains uneven, reactive, and falls short of tackling with this novice form of white collar crime. Despite multiple overlapping regulations and rules, enforcement often fall short of holding the correct parties accountable or proactively identifying laundering through digital payment channels.

At present, payment gateways and aggregators are governed primarily by the Payment and Settlement Systems Act, 2007[7], administered by the Reserve Bank of India (RBI). The Act empowers the RBI to regulate entities involved in the processing and settlement of electronic payments. Subsequently, the RBI Guidelines for Payment Aggregators and Payment Gateways (2020, updated in 2021)[8] laid down the conditions for authorization, capital requirements, merchant due diligence, KYC compliance, and grievance redressal for these intermediaries.

While these guidelines do mandate that payment aggregators perform KYC checks on merchants, undertake periodic risk-based reviews, and report suspicious transactions, the compliance burden is often treated as a mere formality. Many entities rely on automated onboarding, which undermines the scope for meaningful scrutiny. Furthermore, there are no criminal penalties prescribed in the RBI circulars for negligent onboarding or failure to detect suspicious merchant activity. Therefore this framework remains administrative and not punitive.

On the criminal side of law, India's single and significant anti-money laundering statute, the Prevention of Money Laundering Act, 2002 (PMLA), criminalizes the act of directly or indirectly attempting to disguise or project proceeds of crime as untainted. However, payment gateway companies , unlike banks or financial institutions, are not currently listed as "reporting entities" under the PMLA, which means they do not have a statutory duty to report suspicious

[7] The Payment and Settlement Systems Act, 2007, Act No. 51 of 2007

[8] *Guidelines on Regulation of Payment Aggregators and Payment Gateways, Reserve Bank of India, RBI/2020-21/117, CO.DPSS.POLC.No.S33/02-14-008/2020-2021 (Mar. 31, 2021), clarifying DPSS.CO.PD.No.1810/02.14.008/2019-20 (Mar. 17, 2020)*

transactions to the Financial Intelligence Unit (FIU-IND)[9]. This creates a dangerous legal blind spot, due to increasing high volumes of potentially illicit financial flows through this route.

Furthermore, while general provisions of the Bhartiya Nyaya Sanhita (BNS)[10], such as Section 316 (cheating)[11], Section 468 (forgery)[12], Section 120B (criminal conspiracy)[13], and Section 409 (criminal breach of trust by agents)[14], may be invoked against individuals or merchants involved in laundering through gateways, they are rarely applied to the payment intermediaries themselves. Courts have not yet evolved jurisprudence around vicarious liability or wilful blindness for fintech platforms in terms of financial crimes.

Alongside, the Information Technology Act, 2000, which governs intermediaries in the digital ecosystem, provides a safe harbour under Section 79[15], protecting intermediaries from liability for third-party content. Payment gateways often invoke this provision to shield themselves from responsibility for the nature of the transactions they process, although they are not "intermediaries" in the traditional sense of content platforms.

Taken in totality, the current legal and regulatory framework suffers from three major gaps: (1) the absence of criminal liability for payment processors facilitating laundering, (2) lack of mandatory reporting obligations under PMLA, and (3) over-reliance on self-regulation and post-facto enforcement. In the absence of statutory recognition of payment gateway laundering as a distinct form of white collar crime, accountability is diffused, and the integrity of digital financial systems remains vulnerable.

Theoretical Classification as White Collar Crime

The concept of white collar crime was introduced by Edwin Sutherland in 1939[16], who defined the same as "crime committed by a person of respectability and high social status in the course of his occupation." Over time, the scope of this definition has expanded beyond individuals to include corporate actors, professional facilitators, and systemic abuse of institutional processes.

[9] *Financial Intelligence Unit-India, Ministry of Finance, https://fiuindia.gov.in/ (last visited Aug. 4, 2025)*
[10] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023
[11] Bharatiya Nyaya Sanhita, 2023, § 316.
[12] Bharatiya Nyaya Sanhita, 2023, § 468.
[13] Bharatiya Nyaya Sanhita, 2023, § 120B.
[14] Bharatiya Nyaya Sanhita, 2023, § 409.
[15] Information Technology Act, 2000, § 79 (India).
[16] Edwin H. Sutherland, White-Collar Criminality, 5 Am. Soc. Rev. 1 (Feb. 1940) (presidential address delivered Dec. 27, 1939).

Payment gateway laundering, though technologically advanced, aligns squarely with the classical and contemporary understanding of white collar crime, particularly as it entails all essentials of the same, it involves deception, financial manipulation, and abuse of legal-economic structures for illicit gain.

At the heart of it, payment gateway laundering involves creating an illusion of legitimate commerce to disguise criminal financial activity. The actors may be faceless tech companies, offshore shell entities, or seemingly innocuous local merchants. However, the underlying conduct, which is routing illegal money through legitimate platforms, is a deliberate and concealed fraud that subverts the transparency and legality of financial systems. The fraud does not involve physical coercion or overt criminality; instead, it is embedded in documentation, digital transactions, and institutional negligence, which are all hallmarks of modern white collar offenses.

Essentially, white collar crime is often facilitated by access to and manipulation of specialized knowledge, infrastructure, or institutional trust. In payment gateway laundering, the perpetrators understand the fintech onboarding process, regulatory thresholds (such as transactions below ₹2,000 often not being flagged) , and how to use tech intermediaries as buffers. The exploitation of loopholes in Know Your Customer (KYC) processes, merchant verification protocols, and refund mechanisms demonstrates a strategic use of institutional systems to commit fraud, are all factors reinforcing its categorization as white collar crime.

Moreover, even if the payment gateway or aggregator is not directly involved in initiating the fraud, its role as a knowing or negligent enabler cannot be ignored. Sutherland's subsequent work on criminological theories such as “organizational deviance” [17]and “neutralization theory”[18] suggests that white collar crime can flourish in corporate cultures where wrongdoing is a habitual, is ignored, or is rationalized. When payment gateways fail to flag evidently suspicious merchants, or turn a blind eye to industry-wide abuse, they may be viewed as complicit via wilful blindness or gross negligence.

In legal theory, white collar crimes are often distinguished not only by who commits them, but by how they are treated within the system it is active in. Offenders in this situation often avoid

[17] Pedro Neves, *Organizational Deviance*, in **The SAGE Encyclopedia of Corporate Reputation** 519–20 (Craig E. Carroll ed., Sage Publ’ns 2016) ci.nii.ac.jp+10novaresearch.unl.pt+10journals.sa
[18] Mark Dziak, *Neutralization Theory*, in **EBSCO Research Starters: History** (2024) (via EBSCOhost).

the calling these acts one with the notion of "criminality" attached to them and enforcement tends to be limited to civil penalties or compliance orders by courts. This applied to payment gateway laundering in India today, where even high-profile cases lead only to temporary freezes or warnings, as opposed to formal charges or convictions. This underscores the classic invisibility and under-penalization of white collar crime, despite its harmful repercussions.

Payment gateway laundering is not a mere regulatory lapse or compliance oversight, it is rather a structurally embedded financial crime that mirrors the deceptive, calculated, and institutionally embedded nature of white collar criminality. Recognizing it as what it traditionally is, is essential. Not only for accurate legal classification but for enabling proportionate enforcement and deterrence.

Challenges in Detection and Enforcement

Despite the growing reported instances of payment gateway laundering, regulatory framework in India faces significant structural and operational hurdles in detection, investigation, and prosecution this form of white collar crime. The lack of technological advancements , cross jurisdictional nature of these acts, and institutional ambiguity surrounding payment intermediaries create a perfect storm that allows such acts to occur with impunity.

One of the foremost challenges is the opacity of digital transactions. Payment gateways process thousands of transactions daily, many of which are micro payments from multiple end users. When such transactions are routed through layered merchant accounts, often tied to different shell companies or proxy entities, it becomes extremely difficult for regulators to trace the source, or beneficiary of suspicious funds without deep forensic analysis. As opposed to traditional banking fraud, which has the potential of leaving evidentiary paper trails or depend on insider testimony, gateway laundering is majorly automated and encrypted, which makes detection inherently complex.

Second, there is an absence of real-time oversight mechanism. While payment aggregators are mandated by the RBI to conduct KYC and periodic merchant due diligence, these obligations are post-facto in nature i.e, the measures are taken post the crime is committed. There is no mandate for continuous behavioural monitoring, nor is there a centralized system for flagging suspicious mercantile activity across platforms. As a result, an individual or entity deplatformed by one gateway for suspicious acts can easily open an account with another using

minorly altered credentials. The lack of a shared fraud intelligence network among fintech platforms and enforcement agencies leads to regulatory void, thereby perpetuating laundering cycles.

Third, enforcement suffers due to institutional overlap and unclear accountability. In India, financial crimes may fall under the jurisdiction of multiple bodies, namely, the Enforcement Directorate (ED) under the PMLA, the RBI for regulatory compliance, the Financial Intelligence Unit (FIU) for suspicious transaction reporting, and local police or cyber cells under the BNS or IT Act. However, these bodies often operate in silos, and there is no cohesive investigative framework for fintech-specific laundering. For instance, The RBI, may impose restrictions or issue advisories but lacks the power to prosecute such criminal tendencies. Parallelly, ED may initiate proceedings only when predicate offences are established, by which time the funds and actors have often vanished, reinforcing the post facto nature of these punitive measures.

Another significant issue is the legal ambiguity surrounding the liability of payment gateways themselves. These entities often claim to be "mere facilitators," thereby seeking shelter under the safe harbour protections under Section 79 of the IT Act, and isolating themselves from the transactions they process. While there is a moral expectation of due diligence, there is no statutory framework that imposes vicarious or criminal liability on payment intermediaries who fail to flag or prevent laundering. This limits the ability of enforcement agencies to pursue the gateway as part of a criminal conspiracy or abetment.

Lastly, the cross-border element of many laundering schemes, such as those involving offshore shell companies, cryptocurrency exchanges, or foreign-controlled apps, adds an extra layer of enforcement complexity. The extra territorial nature of the crimes, poses significant questions as to the jurisdiction within which they may be tried. Mutual Legal Assistance Treaties (MLATs) and international cooperation mechanisms often work at a turtle pace, which makes MLATs in general ineffective for time sensitive financial investigations and penalisation.

Recommendations and Policy Suggestions

As discussed throughout, Payment gateway laundering is a complex and evolving threat that cannot be addressed by piecemeal regulation or reactive enforcement. Given the digital, decentralized, and multi-party nature of the laundering process, a comprehensive response is

necessary, especially one that spans regulatory, institutional, technological, and international dimensions. Let us categorically discuss a few detailed recommendations to equip the Indian regime to better detect, deter, and prosecute payment gateway laundering as a form of white collar crime.

Firstly, mandating Real-Time Monitoring and AI-Driven Surveillance Systems could be beneficial. The stagnant nature of current compliance mechanisms, such as initial KYC and quarterly reviews, is wholly inadequate in the face of sophisticated laundering operations. The RBI, in coordination and collaboration with the Ministry of Electronics and Information Technology (MeitY), must issue binding guidelines which would require all licensed payment gateways to implement real time monitoring frameworks powered by AI and machine learning algorithms. These systems must be capable of, a) Detecting abnormal transaction volumes or frequencies relative to industry peers, b) Mapping transaction origin-destination trails to spot circular transfers, c) Flagging inconsistent metadata such as mismatched IP geolocation, high-risk devices, or VPN routing, d) Auto-suspending merchant accounts until anomalies are reviewed manually. These AI systems can evolve over time using supervised learning based on historical fraud cases, thus becoming more effective with usage. Moreover setting up a statutory body for oversight of these AI checks, could create a check and balance system, creating a symbiosis between human and technology, as well as an additional layer of security. Additionally, RBI's supervisory tech initiative (SupTech) could be leveraged to build a centralized dashboard to aggregate red flags from across fintech platforms.

Secondly, establishment of a Centralized Merchant Due Diligence & Monitoring Registry, is suggested. Currently, malicious actors exploit merchant onboarding systems across gateways by submitting slightly altered documentation to different platforms. To prevent this, a National Merchant Verification Repository (NMVR) is recommended, linking Aadhaar, PAN, and GSTN, and integrated into DigiLocker APIs. Key features of this system could include a) Mandatory digital onboarding through the NMVR portal, b) Visibility into historical transaction patterns, risk scores, and blacklisting records, c) Authentication of ultimate beneficial ownership (UBO), especially for private limited and LLP entities, d) Cross-gateway flagging if the same director or PAN is associated with a suspicious account. Payment gateways should be required to perform real-time API checks with this registry before settling any merchant payments.

Thirdly, reformation of Legal Liability Framework for Payment Gateways could prove to be beneficial. The current invocation of Section 79 of the IT Act by payment processors to deny responsibility is no longer tenable. Parliament should consider creation of a Fintech Intermediary Liability Code, which would help assign definition to terms such as

- When payment gateways are "intermediaries" and when they act as "facilitators" or "co-processors" while also assigning them duties,

- A layered liability model with civil liability for negligence, administrative liability for failure to report, and criminal liability for wilful facilitation,

- Mandatory appointment of a Compliance and Risk Officer accountable for reporting under the PMLA and IT Act and preparing due diligence reports.

Akin to how social media intermediaries have graded responsibility under the IT (Intermediary Guidelines) Rules, 2021[19], fintech players should be held to a similar standard of "know-your-client's-business" (KYCB), and not just a standard KYC.

Fourthly, creation of a Fintech Financial Crime Enforcement Task Force. India would benefit greatly by establishing a specialized, multi-agency task force to tackle such financial crimes. This should be an empowered statutory body, backed up by the Ministry of Home Affairs (MHA) or the Ministry of Finance, comprising representatives from Enforcement Directorate (ED), Financial Intelligence Unit (FIU), RBI, SEBI (in cases involving securities fraud), MeitY (for digital compliance enforcement) and State cybercrime units. The task force should be provided with its own budget, digital forensic capacity, and legal mandate to initiate joint investigations, share intelligence in real time, and coordinate cross-border probes through Interpol and FATF channels.

Fifthly, it is suggested to tighten Escrow and Fund Settlement Guidelines for High-Risk Merchants. The RBI already mandates escrow accounts [20]for payment aggregators. However, this should be tightened for high-risk merchants through:

[19] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, India.
[20] Castler, *RBI Guidelines 2025: How Escrow Is Becoming the Gold Standard for Transactional Security*, Castler Learning Hub (2025), https://castler.com/learning-hub/rbi-guidelines-2025-how-escrow-is-becoming-the-gold-standard-for-transactional-security.

- Tiered fund release models, where higher-risk categories (e.g., crypto-related services, digital gaming, adult content, unregulated consultants) face delayed settlements (e.g., T+7 or T+15 days);

- Randomized audits of settlement trails for flagged merchants;

- Mandatory disclosures of sector category and business model to the gateway, with penalty for misclassification.

Taking such proactive steps at an early stage would help break the money laundering process before the illegal funds can be withdrawn or moved to another account or location.

Sixthly, strengthening of Cross-Border Investigative Capacity. Payment gateway laundering often involves international digital trails, especially when foreign shell companies or crypto exchanges are used. Therefore, it is recommended that India should -

- Upgrade its international cooperation mechanisms under MLATs, TIEAs (Tax Information Exchange Agreements), and FATF obligations;

- Create a Digital Asset Tracking Cell within ED/FIU specifically to trace crypto-to-fiat laundering routes via payment processors;

- Push for data-sharing agreements with major jurisdictions, especially Singapore, the UAE, and Mauritius, which are common conduits for payment laundering.

Moreover, India should encourage fintech platforms with cross-border operations to retain mirror data servers in India and disclose end-to-end transactional metadata.

Lastly, A self-regulatory organization (SRO) of payment aggregators and gateways, which would be registered with the RBI, should be encouraged in order to –

- Establish a Code of Conduct for Merchant Risk Scoring and Fraud Response;

- Maintain a shared fraud database akin to how CIBIL maintains credit histories;

- Conduct third-party certification of compliance systems annually.

This would ensure that fintech innovation does not come at the cost of financial integrity and that peer monitoring helps lift sector-wide standards.

Conclusion

The phenomenon of payment gateway laundering lurks in the shadows and represents a quiet yet deeply concerning evolution in the landscape of white collar crime. Powered by the rapid growth of fintech infrastructure and the opacity of digital transactions, criminals are now able to exploit trusted financial intermediaries to move illicit funds under the cover of legitimacy. This form of laundering is difficult to detect, technologically sophisticated, and legally ambiguous, often escaping both enforcement scrutiny and regulatory reach.

What sets payment gateway laundering apart is not just its novelty, but the way it undermines institutional trust in digital finance. It exposes critical gaps in existing legal frameworks, particularly regarding intermediary liability and the enforcement of anti-money laundering norms in the online payments space. While fintech has undoubtedly democratized financial access and convenience, it has also created new vulnerabilities that traditional regulatory tools are ill-equipped to address.

Recognizing and naming this form of laundering is the first step. As the digital economy continues to evolve, so must our understanding of crime within it, especially when it wears the mask of innovation and operates through the very channels designed to promote financial transparency.