CROSS-BORDER CONSUMER PROTECTION IN E-COMMERCE: EVALUATING THE EFFECTIVENESS OF LOCAL CONSUMER LAWS AGAINST FRAUDULENT INTERNATIONAL SELLERS

by

Riya Sinha,
Guest Faculty,
Department of Commerce, Ambedkar College, Fatikroy

ABSTRACT

The rapid proliferation of global e-commerce has fundamentally transformed consumer behavior, enabling seamless transactions across international borders. However, this digital expansion has simultaneously exposed consumers to heightened risks of cross-border fraudulent practices, including non-delivery of goods, counterfeit products, and deceptive marketing. This paper evaluates the operational effectiveness of domestic (local) consumer protection laws when applied to fraudulent international sellers, with a dedicated focus on the evolving Indian regulatory landscape. By examining jurisdictional hurdles, choice-of-law dilemmas, and the systemic challenges of cross-border enforcement, the research highlights a critical regulatory gap. While domestic frameworks—such as India's Consumer Protection Act, 2019, the EU's Consumer Rights Directive, or the US Federal Trade Commission guidelines—offer robust internal protections, their extraterritorial enforcement remains severely limited. The study analyzes the pivotal role of international cooperation frameworks alongside specific Indian statutory provisions, concluding that safeguarding the digital marketplace requires a shift from isolated local legislation to harmonized international enforcement mechanisms and decentralized, tech-driven dispute resolution platforms.

Keywords**:** Cross-Border E-Commerce, Consumer Protection, Online Fraud, Extraterritorial Jurisdiction, Conflict of Laws, Indian Consumer Law, Consumer Protection Act 2019.

---

1. Introduction

The global e-commerce marketplace operates as a borderless ecosystem, yet it remains tethered to a fragmented web of domestic legal jurisdictions. Driven by advancements in digital payment systems, global logistics, and algorithmic marketing, cross-border e-commerce has grown exponentially over the past decade. While this shift offers consumers unprecedented access to global goods, it has also created a fertile environment for unscrupulous international entities. Fraudulent sellers exploit the spatial and legal distances between themselves and consumers, frequently engaging in identity theft, selling counterfeit items, or disappearing entirely post-transaction.

This vulnerability is borne out in complaint data collated by India's Department of Consumer Affairs: grievances against e-commerce companies registered with the National Consumer Helpline rose from roughly eight per cent of all complaints four years earlier to nearly forty-eight per cent by November 2022, with total monthly complaint volumes more than doubling from about 40,000 to 90,000 over the same period.[1] While such figures capture domestic as well as cross-border disputes, they nonetheless indicate the scale of consumer harm that existing redressal mechanisms are increasingly called upon to absorb.

When a consumer suffers financial harm within a purely domestic transaction, local consumer protection agencies and national laws provide relatively straightforward mechanisms for restitution. However, when the merchant is located overseas, the protective umbrella of local legislation begins to fracture. Consumers face a daunting maze of conflicting regulations, high costs of cross-border litigation, and language barriers.

This descriptive research paper evaluates how effectively local consumer laws protect buyers from fraudulent international sellers. It explores the structural legal vulnerabilities inherent in cross-border digital trade, evaluates the limitations of national regulatory bodies, and deeply analyzes how developing frameworks—specifically within India—attempt to address these borderless legal challenges.

2. Jurisdictional Challenges and Conflict of Laws

The primary obstacle in protecting domestic consumers from international fraud lies in the doctrine of state sovereignty and the territorial limitations of law.

[1] 'E-Commerce Complaints on National Consumer Helpline More than Double to 90,000 in a Month' IndiaRetailing (New Delhi, 19 December 2022) <https://www.indiaretailing.com/?p=167216> accessed 18 September 2026.

2.1 Establishing Jurisdiction

For a local court or regulatory body to penalize a fraudulent entity, it must first establish jurisdiction over that entity. Under traditional private international law, jurisdiction is heavily tied to physical presence or the place where the contract was formed. In digital trade, determining where an online transaction actually takes place is notoriously complex:

- **Targeting Tests:** Some jurisdictions apply a "targeting test" (e.g., the European Union's Brussels Ibis Regulation). If an international seller actively targets consumers in a specific country—by using their local currency, language, or top-level domain—the local courts may claim jurisdiction.
- **The "Passive" Website Defense:** Fraudulent sellers often argue that their website is passive and globally accessible, meaning they did not explicitly target the victim's specific jurisdiction, thereby dodging local legal reach.

Indian courts confronted with comparable disputes have tended to apply an analogous standard, sometimes described as a purposeful availment or targeting test. Commentary on this line of jurisprudence notes that the mere accessibility of a foreign website within India is not, by itself, sufficient to found jurisdiction; a plaintiff must instead demonstrate that the website's operators purposefully and substantially directed their commercial activity toward the Indian market.[2] This mirrors the difficulty identified above, since fraudulent sellers can just as easily argue that their platform is passively accessible rather than actively targeted at Indian consumers.

2.2 Choice of Law Dilemmas

Even if a domestic court claims jurisdiction, it must determine *which* country's laws apply to the dispute.

- **Terms of Service (ToS) Exploitation:** Fraudulent operators frequently embed "Choice of Law" clauses within complex, non-negotiable online terms of service. These clauses mandate that any dispute must be governed by the laws of a foreign jurisdiction—often a regulatory haven with weak consumer protections.
- **Mandatory Local Rules:** While many nations possess mandatory consumer protection rules that override foreign contract clauses to protect their citizens, enforcing these rules against a

---

[2] Manisha Singh and Dheeraj Kapoor, 'India: Protection of IP Dwindles at the Border' Conventus Law (2021) <https://conventuslaw.com/report/india-protection-of-ip-dwindles-at-the-border/> accessed 18 September 2026.

bad actor with no physical or financial assets in the consumer's home country is practically impossible.

3. The Indian Legal Landscape: Statues and Pitfalls

India has taken progressive legislative strides to modernize its digital consumer safety nets. However, the realities of cross-border e-commerce continue to stretch the limits of these statutes.

3.1 The Consumer Protection Act, 2019 and E-Commerce Rules, 2020

The **Consumer Protection Act, 2019 (CPA 2019)** replaced an outdated 1986 law to specifically address the digital boom. Crucially, the Consumer Protection (E-Commerce) Rules, 2020 expanded its reach:

- **Extraterritorial Intent:** The rules explicitly apply to all e-commerce entities selling goods or services to consumers in India, regardless of whether they are registered or located in India.
- **Nodal Officer Mandate:** Foreign e-commerce entities targeting Indian consumers are legally required to appoint a nodal person of contact or an entity in India to ensure compliance and handle grievances.
- **Central Consumer Protection Authority (CCPA):** CPA 2019 established the CCPA as a central regulator with the power to investigate violations, recall unsafe goods, and issue penalties for misleading advertisements. Between 2020 and early 2026, this enforcement machinery translated into concrete outcomes: the Ministry of Consumer Affairs has reported that 997 notices were issued to e-commerce platforms for unfair practices and that refunds amounting to approximately ₹1,440 crore were facilitated for aggrieved consumers as a result.[3] This record demonstrates that the CCPA's authority, while considerable, has so far been exercised predominantly against platforms and sellers that maintain a presence within India.

3.2 The Information Technology (IT) Act, 2000

While CPA 2019 handles commercial grievances, cyber-fraud elements are governed by the Information Technology Act, 2000.

[3] 'CCPA Acts Against E-Commerce Violations, Issues Notices for Unfair Practices' News on AIR (New Delhi, 18 March 2026) <https://www.newsonair.gov.in/ccpa-acts-against-e-commerce-violations-issues-notices-for-unfair-practices> accessed 18 September 2026.

- **Section 75** of the IT Act explicitly grants extraterritorial jurisdiction over offenses committed outside India, provided that the offense involves a computer, system, or network located inside India.
- **Section 79** grants intermediaries, including global marketplaces operating in India such as Amazon and Flipkart, a conditional safe harbour from liability for third-party content rather than an obligation to actively police listings. This immunity is contingent on the intermediary exercising due diligence and acting to remove or disable unlawful listings once it receives actual knowledge through a court order or a government notification, a due-diligence framework substantially elaborated by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[4]

3.3 The Failure of Enforcement Against Foreign Rogue Sellers

Despite these robust domestic laws, India faces steep challenges when a foreign vendor operates independently (without a large marketplace intermediary):

1. **Lack of Physical Assets:** If a fly-by-night operator located in Eastern Europe or Southeast Asia scams an Indian citizen, the CCPA cannot easily enforce penalties or execute an order if the seller has no physical presence or assets within Indian borders.
2. **The "Nodal Officer" Loophole:** Rogue websites operating entirely outside India completely ignore the requirement to appoint a domestic nodal officer. The Indian government's primary recourse is to issue a site-blocking order under Section 69A of the IT Act, which protects *future* consumers but does nothing to retrieve the lost funds of the initial victims.

This asymmetry is visible in the CCPA's own enforcement record. Its most prominent orders and penalties to date, including those against Amazon, Flipkart, Meesho and Snapdeal, have consistently targeted platforms and sellers with a registered presence or commercial footprint in India; refunds and penalties facilitated in e-commerce grievances alone were reported at ₹36.8 crore since April 2025.[5] Independent overseas sellers with no comparable footprint

[4] Ashima Obhan, 'Intermediary Safe Harbour' Law.asia (7 April 2024) <https://law.asia/intermediary-safe-harbour/> accessed 18 September 2026; Alnoor Peermohamed and Romita Majumdar, 'End of Era! eBay India's 14-Year Long First Innings Comes to an End' ThirdEyeSight (26 July 2018) <https://www.thirdeyesight.in/?p=5771> accessed 18 September 2026.

[5] 'CCPA Fines Amazon, Flipkart, Meesho and Meta ₹10 Lakh Each Over Illegal Walkie-Talkie Listings' Storyboard18 (11 February 2026) <https://storyboard18.com/how-it-works/ccpa-fines-amazon-flipkart-meesho-and-meta-%e2%82%b910-lakh-each-over-illegal-walkie-talkie-listings-89370.htm> accessed 18 September 2026.

rarely feature in these proceedings, which illustrates in practice the jurisdictional limits described above.

4. The Global Enforcement Gap of Local Consumer Laws

The ultimate measure of a law's effectiveness is its enforceability. Local consumer protection mechanisms—ranging from India's District Consumer Disputes Redressal Commissions to the US Federal Trade Commission (FTC)—face severe systemic limitations across borders.

4.1 Lack of Extraterritorial Extent

A domestic judgment ordering a fraudulent overseas seller to refund a consumer is largely a "paper tiger." National regulators cannot dispatch enforcement officers across international borders to seize assets or close down businesses. Without a reciprocal treaty or bilateral enforcement agreement between the consumer's country and the seller's country, the judgment cannot be executed.

4.2 Anonymity and the Jurisdictional Veil

Fraudulent sellers routinely exploit the anonymity of the internet. They use virtual private networks (VPNs), shell companies registered in tax havens, drop-shipping models, and spoofed domains. By the time a local consumer protection agency investigates a complaint, the seller has often deactivated the website, moved their digital assets, and re-emerged under a different corporate alias in an entirely different country.

4.3 The Financial Inequity of Redress

For individual consumers, the financial loss from online fraud is typically low-to-moderate (e.g., ₹5,000 to ₹50,000). The cost of hiring international legal counsel, translating documents, and navigating cross-border judicial processes vastly exceeds the value of the scammed transaction. Consequently, the vast majority of cross-border consumer fraud goes unreported and unprosecuted. This mismatch is reflected in official complaint data, where refunds facilitated by consumer authorities for e-commerce grievances have tended to be measured in the tens of crores of rupees in aggregate rather than in large sums per individual case, underscoring that the typical fraud victim's claim is simply too small to justify the transactional cost of cross-border legal recourse.[6]

5. International Frameworks and Cooperative Mechanisms

Recognizing the limitations of localized laws, international bodies have attempted to build collaborative networks to combat global e-commerce fraud.

Framework/Organization	Primary Function	Limitations
ICPEN (International Consumer Protection and Enforcement Network)	Facilitates cross-border information sharing and joint law enforcement actions among 70+ nations.	Functions primarily as a cooperative network; lacks binding legislative or sanctioning power.
UNCTAD (United Nations Conference on Trade and Development)	Provides guidelines for consumer protection, urging member states to harmonize e-commerce laws.	Guidelines are non-binding recommendations; adoption depends entirely on voluntary national implementation.
OECD Guidelines for Consumer Protection in E-Commerce	Recommends minimum standards for transparency, fair marketing, and cross-border dispute resolution.	Primarily influential among developed nations; often ignored by rogue operators in unregulated jurisdictions.

India participates directly in this cooperative architecture: the Department of Consumer Affairs is a listed member of ICPEN, alongside consumer protection authorities from over seventy other jurisdictions.[7] This membership allows Indian regulators to exchange intelligence on cross-border scams and take part in coordinated enforcement sweeps, even though, as the table above indicates, ICPEN itself possesses no independent power to compel a foreign seller's compliance.

While these frameworks have improved information sharing and occasionally led to coordinated sweeps against massive international scam networks, they lack the immediate, binding authority required to protect day-to-day individual transactions.

[6] Storyboard18 (n 6).

[7] International Consumer Protection and Enforcement Network, 'Who We Are' (icpen.org) <https://www.icpen.org/node/10> accessed 18 September 2026.

6. Alternative Mechanisms: The Shift to Soft Law and Private Governance

Because public international law is slow to adapt, the burden of protecting cross-border consumers has increasingly shifted toward private entities and technological solutions:

- **Chargeback Protocols (RBI Mandates):** Financial bodies like the Reserve Bank of India (RBI) have reinforced consumer-centric mandates for cyber fraud. Under international network rules (Visa, Mastercard), consumers can initiate a "chargeback" through their issuing banks, providing a swift extra-judicial mechanism to reverse transactions with fraudulent international parties.
- **Online Dispute Resolution (ODR):** Major global marketplaces utilize automated, decentralized ODR platforms to resolve disputes. These systems leverage escrow payments—holding funds until the consumer verifies delivery—effectively mitigating fraud before the seller can access the cash.

7. Comparative Analysis of Payment Authentication: India's Rigid KYC & 2FA vs. Western Models

7.1 India's Regulatory Sandbox: Rigid KYC, DigiLocker, and Mandated 2FA

The Reserve Bank of India (RBI) approaches digital transactions with a strict "fraud prevention first" philosophy. This has resulted in a heavily regulated, structural payment environment:

- **Mandatory Two-Factor Authentication (2FA):** Unlike many Western systems that allow "one-click" checkouts based purely on saved card details, the RBI mandates a strict Multi-Factor Authentication (MFA) protocol. Every digital domestic transaction requires a second layer of verification, traditionally an instantaneous Time-based One-Time Password (TOTP) sent via SMS or authenticated through an app.
- **Centralized, Biometric-Backed KYC:** India's Know Your Customer (KYC) mandates are among the tightest globally, anchored by the Aadhaar (UIDAI) biometric database and permanent account numbers (PAN). The widespread legal validation of e-KYC and DigiLocker documentation ensures that every domestic merchant account is linked directly to a verifiable legal identity or individual.
- **The Cross-Border Friction:** While these laws protect consumers domestically, they create immense friction during international purchases. Foreign rogue sellers operating outside of Indian payment rails do not support the RBI-mandated 2FA protocols. When an Indian

consumer enters card data into an unaligned overseas site, the transaction is processed via a standard external clearinghouse without the second security layer, entirely bypassing India's domestic financial safety perimeter. This specific gap has since been addressed at the regulatory level: in September 2025 the RBI issued the Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025, which for the first time require card issuers to validate an additional factor of authentication for non-recurring cross-border card-not-present transactions whenever requested by the overseas merchant or acquirer, with compliance mandated from 1 April 2026.[8] The effectiveness of this extension will nonetheless depend on voluntary participation by overseas merchants and acquirers, since the RBI cannot compel a foreign entity outside its regulatory perimeter to raise such a request.

7.2 The Western Model: Frictionless Commerce and Risk-Based Authentication

In contrast, markets like the United States prioritize economic velocity and user-experience friction reduction, relying heavily on private governance to clean up fraud post-facto:

- **Risk-Based Authentication (RBA):** Rather than mandating an algorithmic blanket step like a OTP for every purchase, Western financial institutions use background behavioral data. They analyze device fingerprints, geographic locations, and past user history. A secondary verification step is only triggered if a transaction looks highly anomalous.
- **Decentralized KYC:** In the US, merchant verification is heavily decentralized, relying on private credit reporting bureaus (Equifax, Experian) and commercial background checks rather than a unified government biometric index.
- **The European Union Exception (PSD3 & 3D Secure):** The EU has moved closer to India’s model through its Payment Services Directive framework, where PSD2 already enforces SCA and a successor package, PSD3 together with a directly applicable Payment Services Regulation, was provisionally agreed upon by the European Parliament and Council in November 2025 but remained pending formal adoption and publication at the time of writing, with application expected only from 2026 or later[9], which enforce Strong Customer Authentication (SCA). Using protocols like 3D Secure 2.0, European banks challenge high-

[8] Ajinkya Kawale, 'RBI Mandates Stronger Two-Factor Authentication in New Guidelines' Business Standard (Mumbai, 25 September 2025) <https://www.business-standard.com/finance/news/rbi-two-factor-authentication-digital-payments-guidelines-2026-125092501154_1.html> accessed 18 September 2026.

[9] Rami Josef, 'An Updated Guide to PSD3 and PSR for Merchants' Checkout.com (29 January 2026) <https://www.checkout.com/blog/guide-to-psd3-and-psr> accessed 18 September 2026.

risk or cross-border transactions natively. However, like India, the enforcement mechanism of SCA breaks down when the transaction terminates with a merchant bank located outside the EEA (European Economic Area).

7.3 The Regulatory Disconnect: Digital Signatures and Fraud Mitigation

Under India's Information Technology Act, 2000, electronic and digital signatures (such as eSign backed by an asymmetric crypto-key pair) carry equivalent legal weight to physical signatures. This provides an absolute chain of custody for domestic contracts.

However, fraudulent international entities exploit the systemic differences between these regions. A rogue vendor can easily register an account with a loosely-regulated European or Caribbean merchant processor using basic documentation, completely evading the stringent identity-verification thresholds mandated by the RBI. Consequently, while an Indian consumer is exceptionally safe when transacting within domestic boundaries, the moment their capital crosses the border, they step into a financial zone where anonymity is easily weaponized by bad actors.

8. Conclusion

Local consumer protection laws are inherently unequipped to independently combat fraudulent international sellers. While domestic frameworks successfully define consumer rights and set high standards for commercial behavior, their efficacy terminates at national borders due to jurisdictional barriers, choice-of-law conflicts, and a profound cross-border enforcement gap.

India's Consumer Protection Act, 2019 serves as an excellent case study of an aggressive statutory design that remains limited by geopolitical realities. Writing extensive extraterritorial jurisdiction into local laws is meaningless without bilateral and multilateral execution mechanisms.

To establish a truly secure global marketplace, the regulatory approach must evolve away from isolated state-centric laws and toward deeply integrated global systems. Future efficacy rests on three pillars: the international harmonization of e-commerce definitions, binding cross-border enforcement treaties that allow national regulators to penalize foreign bad actors, and the expanded integration of tech-driven private safeguards like blockchain-verified escrows and unified Online Dispute Resolution (ODR) platforms.

References

- Central Consumer Protection Authority (CCPA). (2020). *Consumer Protection (E-Commerce) Rules, 2020*. Ministry of Consumer Affairs, Food and Public Distribution, Government of India.
- European Parliament and Council. (2011). *Directive 2011/83/EU on consumer rights*. Official Journal of the European Union.
- Federal Trade Commission (FTC). (2020). *Protecting Consumers in the Modern Marketplace: Cross-Border Fraud and Enforcement Report*. FTC Bureau of Consumer Protection.
- Government of India. (2019). *The Consumer Protection Act, 2019*. Gazette of India.
- Ministry of Electronics and Information Technology (MeitY). (2000). *The Information Technology Act, 2000*. Government of India.
- OECD. (2016). *Consumer Protection in E-commerce: OECD Recommendation*, OECD Publishing, Paris.
- United Nations Conference on Trade and Development (UNCTAD). (2017). *United Nations Guidelines for Consumer Protection*. United Nations Publication.
- European Commission. (2023). *Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market (PSD3)*. Official Journal of the European Union. (COM(2023) 366 final). European Commission, Brussels. Status as of the time of writing: provisionally agreed by the European Parliament and Council in November 2025; not yet formally adopted or published.
- Reserve Bank of India (RBI). (2021). *Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated 2021)*. RBI Department of Regulation.
- Reserve Bank of India (RBI). (2023). *Framework for processing of e-mandates for recurring online transactions*. RBI Payment and Settlement Systems.