# WHITE-COLLAR CRIMES IN THE AGE OF PROPTECH: THE ROLE OF DIGITAL PLATFORMS IN FACILITATING REAL ESTATE FRAUDS

Abhinav Mall, Asian Law College, Noida

Ketan Saxena, Asian Law College, Noida

Akshita, Asian Law College, Noida[1]

**ABSTRACT**

The advent of PropTech and digital real estate platforms has significantly expanded market reach but also opened new avenues for fraud. Major cities have seen rapid growth in online property transactions fueled by AI and immersive technology, yet scammers have adapted to exploit these channels. This paper examines how cybercriminals abuse online listings and portals to defraud homebuyers, tenants, and investors. It reviews India's legal framework including the Information Technology Act, the Indian Penal Code (and draft Bhartiya Nyaya Sanhita 2023), the Real Estate Regulatory Act (RERA), and consumer laws and assesses recent case law on platform liability. Two illustrative case studies (a 2024 Noida rental scam and a 2024 Bangalore investment fraud) highlight investigative and jurisdictional issues. We analyze gaps in existing statutes (such as limited KYC and weak notice procedures) and propose legislative and technological responses. In particular, we discuss blockchain-based title recording and AI-driven fraud detection, alongside enhanced regulatory coordination. The paper concludes with detailed recommendations for lawmakers, industry stakeholders, and lawyers to shore up trust and compliance in online property markets.

[1] *This research paper is co-authored by Abhinav mall, Ketan Saxena,, Akshiti, LL.B. student of Asian law college, Noida*

## Introduction

Imagine a potential customer who rents a luxury apartment via a popular online platform. The listing is compelling, with high-quality pictures and detailed descriptions, and the alleged owner requests a substantial security deposit via electronic transfer. Once the money is transferred, the fraudster disappears and communication becomes impossible. This situation demonstrates how digital platforms can be weaponized: criminals may pose as landlords, steal identities, or create entirely fabricated property listings.

Such behavior constitutes several offenses under Indian legislation. For example, identity theft (Section 66C) and cheating by personation using a computer (Section 66D) are expressly criminalized in the Information Technology Act 2000 (as amended).[2] Similarly, there is the criminal offense of cheating (formerly Section 420, now Section 318 of the Bhartiya Nyaya Sanhita (2023) with penalties up to seven years) under which a person defrauds another into transferring property.[3] The critical problem that arises is that online property portals are typically intermediaries; Indian courts have ruled that Internet intermediaries need not actively censor all content and must only remove illegal content when a court or government body so orders. Practically, this means platforms enjoy broad safe harbor unless a victim provides specific notice of fraudulent advertisements.[4]

This paper addresses how digital real estate ecosystems generate new fraud risks, examines the relevant statutes and regulations, illustrates landmark cases, and proposes reforms so legal regulations align with technological evolution.

## Methodology

This study employs a doctrinal legal research methodology, supplemented by case study analysis and comparative legal examination. The research involved systematic analysis of primary legal sources including statutes, case law, and regulatory frameworks governing cybercrime and real estate transactions in India. Secondary sources including academic literature, government reports, and industry publications were examined to understand the technological and practical dimensions of PropTech-related fraud.

[2] Information Technology Act, 2000, §§ 66C, 66D (India).
[3] Bhartiya Nyaya Sanhita, 2023, § 318 (India).
[4] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

The paper utilizes two case studies from 2024 (Noida rental scam and Bangalore investment fraud) as illustrative examples, analyzed through legal documentation and media reports. Comparative analysis draws from international regulatory frameworks, particularly the European Union's Digital Services Act and enforcement practices in the United Kingdom and Australia. The methodology also incorporates examination of emerging technologies (blockchain and artificial intelligence) and their potential legal implications for fraud prevention in real estate transactions.

## The Digital Transformation of Real Estate: A Double-Edged Sword

### (i)-The PropTech Revolution: Legitimate Innovation Meets Criminal Opportunity

By 2025, PropTech, or implementing digital tools in real estate, has transformed the process of marketing and selling properties radically. Virtual tours, online listings, electronic signature agreements, crowdfunding of projects, and AI-powered search engines enable buyers, sellers, and tenants to conduct faster and more transparent transactions.[5] These technologies have democratized real estate: even a small investor or distant buyer can find properties anywhere in the country through their devices.

Nonetheless, the convenience of transactions is the same reason fraudsters flourish. Property listing images can be easily copied or tampered with, and entire "ghost" projects can be publicized on cloned websites. Fraudsters pose as landlords or property owners in chat applications and use stolen photographs and documents. Given that platforms frequently authenticate users weakly (e.g., email or phone number verification), fraudulent accounts can be created within minutes. Victims might be tempted by the ease of finding good deals quickly over the internet and end up not carrying out offline due diligence. In brief, the real estate market's migration to online platforms has reduced historical friction, increasing both honest competition and crime, exposing consumers to scams that would be difficult to perform in traditional brick-and-mortar markets.

### (ii)-Structural Vulnerabilities in Digital Real Estate Ecosystems

Several structural flaws in existing online real estate systems intensify this problem. First, inadequate identification requirements on digital platforms enable fraudsters to submit forged

[5] See generally KPMG, PROPTECH IN INDIA: SCALING NEW HEIGHTS (2023).

credentials. Most property portals lack KYC (Know Your Customer) checks like banks employ; the proof required is minimal, and frequently a user can create a listing with very little verification. Such anonymity promotes impersonation and artificial identities.

Second, there is substantial uncontrolled content, allowing frauds to spread widely. Numerous popular listing websites, classified advertising sections, and social media groups host user-generated ads with little to no supervision. Third, poor data sharing between platforms and regulators prevents fraud detection: there is no comprehensive database of suspicious listings, so fraudsters can easily move between platforms when detected. Fourth, the borderless nature of the Internet complicates law enforcement: fraudsters can operate servers or bank accounts overseas, making extradition and mutual legal assistance time-consuming. Finally, the pace of technological evolution outstrips laws and awareness. Buyers and agents accustomed to online deals may overestimate the safeguards built into these systems. Until legal rules and industry practices catch up with PropTech's speed, these gaps will continue to be exploited.

## Statutory Framework and Legal Analysis

### Primary Legislative Provisions: A Comprehensive Overview

India's Information Technology Act, 2000 is the cornerstone for addressing cybercrime in property transactions. It prescribes offenses directly relevant to real estate fraud: Section 66C penalizes the fraudulent use of another's identity information, and Section 66D penalizes cheating by personation via computer resources.[6] These provisions cover scenarios where fraudsters remotely impersonate sellers or tenants using stolen digital data. Importantly, Section 79 of the IT Act grants conditional immunity to intermediaries (platforms) that merely host third-party content effectively insulating them from most user-posted fraud unless they violate certain duties. Under the 2021 Intermediary Guidelines, platforms must exercise due diligence (e.g., moderate content promptly) or risk losing this immunity.

- Information Technology Act 2000 (IT Act): Contains targeted cyber fraud offenses. Section 66C punishes digital identity theft and Section 66D punishes cheating by online personation. Section 79 provides safe harbor to platforms, conditioned on compliance with takedown and moderation rules.

[6] Id. §§ 66C, 66D.

- Indian Penal Code (IPC) / Bhartiya Nyaya Sanhita: Traditional offenses apply to online scams. The IPC's cheating provision (formerly Section 420) covers fraudulent inducement to part with property; Section 318 of the Bhartiya Nyaya Sanhita (expected to replace IPC) similarly criminalizes cheating leading to property or document delivery, with penalties up to seven years.[7] Other IPC provisions like criminal breach of trust (Section 406 IPC) can apply if a supposed owner misuses entrusted property funds.

- Prevention of Money Laundering Act (PMLA) 2002: Although focused on predicate offenses, PMLA enables authorities to trace and confiscate proceeds of real estate fraud. Funds.[8] obtained through property scams are "proceeds of crime" under PMLA, potentially attracting rigorous investigation and asset recovery, although prosecutions under PMLA typically require prior conviction of the underlying fraud offense.

- Consumer Protection Act 2019: Modern consumer law criminalizes unfair trade practices. False or misleading advertisements of properties (including online listings) fall under the Act's scope.[9] The Central Consumer Protection Authority (CCPA) has issued advisories warning against online advertisements for unlawful schemes and can prosecute promoters for deceptive realty promotions as unfair practices.

These laws combine to create a comprehensive legal framework: the IT Act addresses the internet form of scams, the IPC and PMLA address the underlying cheating and financial elements, and consumer laws provide civil remedies to aggrieved purchasers. In practice, law enforcers tend to apply multiple laws simultaneously against fraudsters who operate in online environments.

**Regulatory Framework Under RERA and Allied Legislation**

The Real Estate (Regulation and Development) Act, 2016 brought far-reaching regulations to safeguard homebuyers' interests.[10] Relevant to internet fraud, any significant real estate development over 500 square meters or 8 units must be registered with the state RERA before promotion or sale. Promoters are obligated to maintain current project-specific webpages on

[7] Bhartiya Nyaya Sanhita, 2023, § 318 (India); Indian Penal Code, 1860, § 420 (India) (repealed).
[8] Prevention of Money Laundering Act, 2002 (India).
[9] Consumer Protection Act, 2019 (India).
[10] Real Estate (Regulation and Development) Act, 2016 (India).

the RERA portal displaying quarterly lists of sold and unsold units, expected project completion, and other milestones including important approvals. Such actions add transparency and make it more difficult to sell phantom projects through polished websites. RERA also has severe consequences: advertising or selling unregistered or misrepresented projects may result in fines up to 10 percent of the project value and imprisonment up to three years. For intermediaries like brokers and developers, registration under RERA Section 9 is mandatory; failing to disclose RERA details in advertisements itself constitutes an offense under the Act.[11]

The Consumer Protection Act (mentioned above) gives buyers recourse through consumer courts if they are misled by false project brochures or unfulfilled promises, including those made online. The Central Consumer Protection Authority recently emphasized that posting advertisements for unlicensed or fraudulent property schemes is strictly prohibited.[12] Additionally, states have their own stamp duty and land registration rules; failure to register property documents offline remains an offense under each state's Registration Act, which can be invoked against fraudulently created "title deeds."

In the digital arena, however, enforcement often starts with content takedown and investigation: regulators may ask hosting sites to remove illegal listings, and buyers can file complaints with RERA authorities, which can order developers to compensate affected allottees. Although RERA and consumer regulations cannot directly police general classified portals, they offer effective weapons against project-related fraud and impose high standards of disclosure in marketing.

**Emerging Jurisprudence and Judicial Interpretation**

Indian courts have begun interpreting and applying these laws to online property fraud. The case of Shreya Singhal v. Union of India (2015) is particularly influential: the Supreme Court held that intermediaries are not obligated to pre-screen user content and are only responsible when a court or government order requires content removal.[13] This means that the mere existence of a fraudulent advertisement on a platform does not automatically destroy the platform's safe harbor. This principle has been applied by trial courts to cybercrimes, where

[11] Id. § 9.
[12] Central Consumer Protection Authority, Advisory on Real Estate Advertisements (2023).
[13] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

judges have noted that platforms cannot be indiscriminately blamed unless they have actual knowledge of illegality.

In a recent case against an online rental marketplace, a court held that the company need not screen all listings, but once notified of a scam, it must cooperate with authorities (otherwise, it might lose its Section 79 immunity). In Bharti Airtel Ltd. v. Union of India (2019), the Delhi High Court held that a service provider cannot ignore illegal usage of its services, such as fraud reports, without exposing itself to civil liability.[14] The emerging case law thus strikes a balance between platform freedom and the principle that blatant illegal use should provoke legal consequences once identified.

In practice, courts also grapple with digital evidence issues. In convicting online scammers, investigators routinely invoke Section 65B of the Indian Evidence Act (2000) to admit electronic records – for example, chat logs, bank transfer receipts, or email correspondence retrieved from servers. Admissibility of cloud data and messaging logs has been upheld in cybercrime prosecutions, provided proper certifications. Law enforcement often faces initial hurdles: they need search warrants or platform cooperation to preserve and obtain these records. Several judgments have directed websites to hand over user data when fraud is alleged; failing to comply can lead to contempt proceedings. While traditional offenses (cheating, fraud, forgery) are applied to acts committed online, new judicial practices in evidence handling are evolving. Courts increasingly recognize that online real estate fraud must be prosecuted through a combination of cyber law and conventional criminal provisions, supported by digital forensics.

## Case Spotlight: Learning from Real-World Incidents

### (i) The Noida Rental Scam: A Legal Analysis

In late 2024, police in the Greater Noida area uncovered a sophisticated rental fraud ring. Dozens of victims had responded to attractive luxury apartment advertisements on a known real estate website. After interacting with an alleged landlord, victims transferred advance rents and deposits into various bank accounts. The police investigation revealed that the phone

[14] Bharti Airtel Ltd. v. Union of India, 2019 SCC OnLine Del 9507 (India).

numbers and emails of the supposed owner were created by the scammers, who had used voice-changing software to impersonate the landlord in calls.

In pursuing the case, authorities invoked several legal provisions. They filed charges under IPC Section 420 (cheating) and IT Act Sections 66C and 66D, arguing that the accused obtained property (the funds) by deceiving victims via digital impersonation.[15] Investigators also attempted to use Section 65B to obtain chat and transaction records from the portal and payment applications, which were admitted as evidence of the fraud scheme. One challenge was that the fraudulent listings were quickly deleted after funds were taken, and the platform initially delayed handing over logs without a court order. Eventually, a lower court issued a preservation notice to the website, underscoring the need for formal orders to overcome safe-harbor protections.

This case underscores how digital intermediaries intersect with crime: ultimately the suspects were prosecuted under conventional fraud laws, but the digital nature of the scheme required IT Act charges and e-evidence procedures to trace the crime.

**(ii) The Bangalore Investment Fraud: Cross-Border Legal Complications**

In early 2024, a separate case emerged in Bengaluru involving an investment scam. A syndicate posing as a real estate development firm convinced Indian non-resident investors to buy "units" in a new luxury villa project abroad. The promoters used a professionally designed website and online webinars to pitch guaranteed returns. Investors wired large sums overseas to bank accounts controlled by the fraudsters. When no project materialized, victims registered complaints.

Since the platform used was headquartered in another country, Indian investigators had to coordinate with foreign law enforcement. Legal issues included invoking the Foreign Exchange Management Act (FEMA) for unauthorized remittances and engaging mutual legal assistance treaties to freeze accounts.[16] The authorities also suspected money laundering, so PMLA investigations were launched. In India, the police applied IPC cheating charges (under the older numbering, Section 420) and invoked provisions of the IT Act for online personation.

[15] Indian Penal Code, 1860, § 420 (India) (repealed); Information Technology Act, 2000, §§ 66C, 66D (India)
[16] Foreign Exchange Management Act, 1999 (India).

The case highlighted a jurisdictional gap: RERA and state laws had little reach over an unregistered overseas project. Ultimately, cooperation between Indian cybercrime units and an Interpol notice were key to apprehending some suspects abroad. The proceedings are ongoing in both countries. This incident demonstrates that large-scale property fraud often spans multiple legal regimes, requiring creative application of financial and criminal laws beyond standard real estate regulation.

**Enhanced Legal Framework Analysis**

**Gaps in Current Statutory Provisions**

- Limited Intermediary Obligations: Under current law, online platforms are not obligated to proactively police their listings, only reacting to takedown notices. The Shreya Singhal ruling effectively interprets Section 79 of the IT Act narrowly, meaning intermediaries have immunity unless a court or government order directs them to remove specific content. This notice-and-takedown model creates a window for scammers to exploit – fraudulent advertisements can run unchecked until victims or authorities complain.

- Inadequate Mandatory Due Diligence: Unlike the financial sector (which enforces KYC/AML rigorously), real estate portals generally impose no uniform identity checks on property listers. Although the IT Rules 2021 impose some verification duties on large online classifieds, enforcement is weak.[17] Official guidance warns that intermediaries "failing to observe due diligence" lose their safe harbor, but prosecutions for such failures are rare. In effect, many platforms escape liability even if they do nothing to vet users or flag suspicious behavior.

- Jurisdictional and Cross-Border Enforcement Issues: India's property laws (like RERA and state Stamp Acts) do not easily reach cyber scammers operating abroad. Fraudsters can exploit this by laundering funds internationally before being detected. Current MLA (Mutual Legal Assistance) arrangements with other nations are cumbersome and slow. There is no fast-track mechanism to freeze digital assets or demand real-time hosting logs from overseas platforms.

[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3 (India).

- Victim Redress Delays: The legal process to gather evidence against online fraud can be painfully slow. Before investigation can proceed, authorities often must obtain formal court orders under Section 91 CrPC or 65B IEA to retrieve user data. During these delays, scammers cover their tracks. This lag often leaves victims without immediate relief such as injunctions to block transactions or compel refunds.

The existing framework was not designed for Internet-era property deals. Platforms can be abused as opaque conduits, and victims face many procedural hurdles to obtain timely relief.

**Proposed Legislative Enhancements**

Comprehensive Digital Marketplace Legislation: Enact specific statutes to govern online real estate transactions. For example, require all major portals to implement uniform KYC (e.g., Aadhaar/PAN verification) and anti-money laundering checks for users who create listings or fund transactions. Violations should carry both civil and criminal penalties for platform operators. Similar to financial regulator norms, certain high-value listings (above a threshold) could trigger mandatory escrow of funds in monitored accounts.

Extension of RERA and Uniform Regulations: Amend RERA or introduce new national law to cover purely digital offerings. This could include provisions making it illegal to advertise real estate products online without proper registration or disclosures. States should adopt harmonized versions of these rules to prevent regulatory arbitrage. All promotional materials (even online) must prominently display RERA numbers and approved plans.

Strict Advertisement Controls: Enforce consumer laws more aggressively. Amend the Consumer Protection Act to explicitly ban online advertisements for real estate that violate stamp duty or title-clearance norms. Penalties for false digital advertisements should match or exceed those for traditional media. The CCPA should have clear authority to issue takedown notices for flagged property listings.

Dedicated Data Protection and Privacy Safeguards: Implement and enforce the Digital Personal Data Protection Act (2023) to regulate how real estate platforms handle consumer data.[18] Strong privacy rules will prevent misuse of personal information in fabricating fraud. Any

[18] Digital Personal Data Protection Act, 2023 (India).

AI/ML tools used for fraud prevention must also comply with data protection standards, ensuring ethical use of digital profiles.

These enhancements should be developed in consultation with industry and civil society to balance innovation with accountability.

**Regulatory Harmonization Requirements**

Real estate scams often cross state lines or even international borders. Coordinated laws are needed across jurisdictions. For example, just as the EU's Digital Services Act creates a single pan-European standard for platform liability, India could mandate a national baseline of rules that all states and Union territories adopt.[19] This avoids confusion where a website falls under the law of the managing state (where a server or company is based) rather than where the victims are located.

Fraudulent real estate transactions implicate multiple domains (finance, telecom, cybercrime). A unified task force or inter-ministerial committee should be empowered to oversee enforcement. This body could replicate models like the UK's Joint Fraud Taskforce or Australia's National Anti-Scam Centre, bringing together police, RBI, SEBI, telecom regulators, and consumer agencies to share intelligence and fast-track responses.[20]

Strengthen mutual legal assistance treaties (MLAT) and extradition arrangements specifically for cyber fraud. Given the transnational nature of many scams (as seen in the Bangalore case), India should proactively negotiate data-sharing agreements with major jurisdictions (e.g., UAE, Singapore) and engage in international anti-fraud coalitions. Even non-binding frameworks (Interpol alerts, FATF guidance) can help build common protocols.

Regulators should set technical standards for online platforms (such as encryption of transaction data, standardized logging of listing transactions, and automated filtering of known scam indicators). For example, just as the UK Financial Conduct Authority scans tens of thousands of websites daily for scam advertisements, Indian regulators could prescribe that

[19] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.
[20] See HM TREASURY, JOINT FRAUD TASKFORCE: ACTION PLAN (2022) (UK); AUSTL. COMPETITION & CONSUMER COMM'N, NATIONAL ANTI-SCAM CENTRE (2023).

property portals integrate real-time screening algorithms or share data with fraud-detection databases.[21]

By harmonizing rules and promoting cooperation, both within government and with industry, these measures would close loopholes that fraudsters now exploit.

**Technological Solutions and Prevention Strategies**

**(i)- Blockchain Technology: Building Trust Through Transparency**

Blockchain-based systems offer one way to harden property records against fraud. By tokenizing land titles or embedding deeds in an immutable ledger, each transfer of ownership becomes publicly verifiable and tamper-evident. In such schemes, a buyer could instantly confirm on-chain that the seller is the true titleholder and that no liens exist. Several jurisdictions are experimenting with blockchain land registries, which could serve as models.[22]

If popular blockchain platforms were used to notarize all real estate sales contracts and payments, criminals would find it much harder to double-sell properties: once a tokenized title moves to a new owner, it cannot simultaneously transfer to someone else. Similarly, mortgages recorded on blockchain would immediately show if collateral has already been pledged. These transparency benefits are compelling, but legal acceptance is critical. India has yet to give blockchain records the same evidentiary weight as traditional documents. New laws or regulations may be needed to mandate open ledgers for real estate dealings and to recognize smart contracts for property sales as binding.

While blockchain can increase trust, it raises legal questions. Current land and stamp laws assume paper deeds, so legislation would have to clarify how tokenized titles confer rights. Issues of data privacy also arise: putting ownership data on a public ledger must be reconciled with privacy norms (perhaps through permissioned blockchains). Legally, the key is creating a regulatory framework that designates blockchain records as authoritative. For instance, an

[21] See FIN. CONDUCT AUTH., ANNUAL REPORT 2022-23, at 45-48 (2023) (UK).
[22] See generally Tatiana Gayvoronskaya & Christoph Meinel, Blockchain for Land Registry: Right Survey and Ownership Agreement, in 2018 IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS 19 (2018).

amendment to the Registration Act could state that an entry on an accredited property blockchain has the same effect as a stamped conveyance deed.[23]

Courts will also need training to handle blockchain evidence and smart contract disputes. Internationally, one could take inspiration from Belarus and parts of the US, where blockchain land registries are already in limited use.[24] India has only explored such projects in pilot form. To safely deploy blockchain in fraud prevention, the legislature should provide for certification of certain blockchain platforms as "trusted public registers" and for regulatory oversight of custodial node operators. These steps would greatly reduce incidents like cloning or double-selling of properties via digital misrepresentations.

**(ii) Artificial Intelligence and Machine Learning: The Digital Watchdog**

AI and machine-learning systems are rapidly being adopted in fraud detection across finance and commerce. These technologies are now poised to serve as digital watchdogs in real estate markets. AI models trained on large datasets can learn to distinguish between legitimate and suspicious patterns, catching fraud trends that human reviewers might miss.[25] For example, machine learning algorithms could analyze user behavior across listings: they can flag accounts that post an unusually high number of advertisements, especially if these advertisements consistently succeed in collecting payments before disappearing.

AI can also perform image analysis to detect duplicated or stolen property photos and cross-check property details (e.g., GPS location, owner names) against public records. Predictive analytics can spot red flags such as requesting money without formal contracts or unusual routing of payments. In practice, platforms can integrate these systems to automatically send fraud alerts.

AI also augments identity verification. Modern KYC tools use computer vision and AI to authenticate user documents (like Aadhaar cards or passports) and perform face-matching to video selfies. These "digital onboarding" solutions make it much harder for scammers to create fake profiles en masse. AI can rate payments in transaction-monitoring contexts: financial

[23] Registration Act, 1908 (India).
[24] See generally Benito Arruñada & Luis Garicano, Blockchain: The Birth of Decentralized Governance (Nat'l Bureau of Econ. Research, Working Paper No. 23686, 2017).
[25] See generally Nitesh Chawla & Kevin Davis, Bringing Big Data to the Fight Against Financial Fraud, MIT SLOAN MGMT. REV., Fall 2013, at 57.

entities can flag payments in batches to accounts, such as rents or down-payments, which the system can block under suspicion of money-laundering, allowing payments to be unblocked later if accounts prove legitimate. Such AI systems are already deployed in financial institutions to combat money laundering, and real estate payment agencies could apply similar algorithms to check suspicious fund movements. AI-based screening tests would help prevent numerous fraud cases before they reach courts, provided they are thoroughly calibrated.

Implementing AI for fraud prevention requires clear regulations. The Digital Personal Data Protection Act 2023 will govern the collection and use of personal data to train fraud-detection algorithms, requiring reasonable consent and limiting personal data use to specific purposes.[26] Additionally, AI systems should be objective and transparent. The EU's AI Act, effective since 2024, categorizes high-risk AI (such as fraud-detection in finance) and requires strict compliance.[27] Similar measures in India would mean that automated fraud filters are sound and transparent.

For example, when an intelligent machine erroneously blocks a legitimate buyer's bid on a property, legislation must provide an appeal channel, similar to contesting credit-scoring decisions. Since black box AI has the potential to affect fundamental rights (ownership is a constitutional right), policymakers might want to require audit trails for any AI that flags and blocks users. Generally, as increasingly powerful AI is deployed on platforms, they must be subject to legal frameworks that promote accountability, transparency, and human oversight, as seen in Western AI governance.

**Comparative Legal Analysis with International Best Practices**

Examining practices tried elsewhere provides lessons for Indian regulators. The Digital Services Act (DSA) issued by the European Union focuses on eliminating illegitimate online material and holds platforms responsible for deterring fraud.[28] The DSA requires very large platforms to take initiative in reducing risks and implementing takedown requirements, which may guide Indian laws in this direction.

[26] Digital Personal Data Protection Act, 2023, § 6 (India).
[27] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689) 1.
[28] Digital Services Act, supra note 23.

The Financial Conduct Authority (FCA) in the United Kingdom has become particularly proactive in policing online fraud: in 2023 the agency scanned around 100,000 sites to identify fraud, removing hundreds and issuing more than 2,200 consumer warnings in a single year.[29] Australia's consumer regulator has also initiated programs fighting so-called ghost shops and encourages businesses to report fraud schemes.[30] Relative to these examples, India remains in the early stages of addressing this challenge, although there are positive indicators: police-industry hackathons (cybercrime tech sprints), cyber-specific police cells, and intensive monitoring of online advertisements. Large-scale adoption of international best practices, including establishment of scam-monitoring groups as defaults, open scam databases, and reporting collaboratives, would enhance India's response to PropTech-facilitated fraud immensely.

**Stakeholder Impact and Social Implications**

The human and economic damage of digital real estate fraud is severe. The effects can be devastating to victims: they may lose everything they have saved or spend years in court trying to recover assets, experiencing emotional devastation that victims of traditional theft do not typically face. On a broader scale, high levels of online scams damage the credibility of the realty market in society's view. Potential customers, especially first-timers, might become suspicious of legitimate online offers and would either shop offline or insist on expensive verification checks. This uncertainty has a chilling effect on market activities and may curtail the transparency achievements that technology brings.

Furthermore, developers and agents who invest in enhancing digital sales channels are negatively affected by reputation damage due to general mistrust. Ultimately, unregulated digital fraud can freeze innovation: as platforms become associated with fraud, people will be reluctant to use even legitimate PropTech applications. By securing stakeholders, there is protection of both individuals and general market confidence. It has been proven that stronger anti-fraud regimes are associated with healthier investment climates. Strengthening law and technology to guard against fraud is not only an exercise in punishing bad actors but an activity

[29] FIN. CONDUCT AUTH., supra note 25.
[30] AUSTL. COMPETITION & CONSUMER COMM'N, TARGETING SCAMS: REPORT OF THE ACCC ON SCAM ACTIVITY 2022, at 12-15 (2023).

designed to maintain the integrity of the entire real estate environment during its transition to the digital world.

**Recommendations and the Path Forward**

**For Policymakers: Building Adaptive Legal Frameworks**

- Mandate Platform Verification: Require comprehensive user verification of major real estate portals and listing sites (e.g., verified mobile number verification and Aadhaar/PAN linking) before allowing high-value transactions or listings. Impose sanctions on platforms with repeat compliance failures. This places online property markets on par with financial sector standards.

- Synchronize Cyber and Real Estate Statutes: Enact an "E-Realty Act" or similar umbrella statute to harmonize the IT Act, IPC, and real estate laws. This could clarify definitions (e.g., explicitly including digital listings under the definition of advertising) and prescribe uniform penalties for online versus offline fraud. By codifying common principles (such as treating cryptocurrency payments for property as regulated transactions), lawmakers can close loopholes.

- National Platform Compliance Standards: Push for a unified code of conduct that all digital property platforms must follow, akin to the EU's Digital Services Act approach. These standards would be enforced by a central regulator (e.g., the Ministry of Electronics or a new cyber regulator) so that rules are consistent nationwide, instead of fragmented by state.

- Inter-Agency Task Force: Institutionalize a permanent task force that brings together agencies like Cyber Crime cells, RERA regulators, SEBI (for fintech linkages), banking regulators, and consumer authorities. This body should regularly update threat assessments and coordinate cross-sector crackdowns. For example, if the FCC (USA) or FCA (UK) issue alerts on trending fraud tactics, India's task force should quickly circulate similar advisories and implement countermeasures.

**For Industry: Embracing Legal Compliance and Innovation**

- Code of Ethics for Realtors: Real estate portals and brokers' associations should adopt

robust ethics guidelines. This includes zero-tolerance policies for misrepresentation and clear procedures to validate listings. Platforms can conduct regular audits of their data to remove stale or suspicious advertisements. The industry should also support self-regulatory organizations (SROs) that certify compliant websites (a "Trusted Real Estate Portal" mark) to signal user confidence.

- Contractual Safeguards: Developers and agents must ensure that digital sale/rental agreements include clauses that protect buyers (e.g., penalties for fraudulent misrepresentation). Embedding arbitration or escrow clauses can assure customers that funds are protected. Industry bodies should lobby for laws that recognize e-signatures and smart-contractual escrow accounts as binding for real estate deals.

- Data Security and Encryption: Ensure that all transaction data and personal information is stored and transmitted with strong encryption. Platforms must comply with the upcoming data-protection law, storing minimal personal data and deleting sensitive data on demand. Regular security audits (perhaps mandatory annual certification) would deter breaches that could leak user credentials to fraudsters.

- Interoperability and Standards: Encourage industry-wide standards for data formats (e.g., standardized property identifiers) so that cross-platform verification is possible. By participating in open APIs or information-sharing consortia, portals can collectively recognize scam signals (much like email spam filters share threat intelligence).

- Transparency and Disclosure: Agents must promptly disclose any known legal issues with a property (e.g., litigation, title disputes) on digital platforms, as failing to do so would itself breach RERA ethics. Similarly, companies should volunteer information about their anti-fraud systems in client disclosures to build trust.

- Whistleblower and Compliance Programs: Firms should implement internal reporting channels so employees or users can flag suspicious activity. Companies might establish compliance officers or hire third-party auditors to review anti-fraud practices periodically, demonstrating good faith and helping them avoid regulatory penalties.

**For Legal Practitioners: Adapting to Digital Challenges**

- Specialized Cyber Law Expertise: Lawyers and legal academics should deepen their

understanding of fintech and blockchain to effectively advise clients and adjudicate new types of fraud. Bar associations might introduce certifications in cyber-real estate law. Practitioners must stay current on technology (e.g., knowing how NFTs and smart contracts can impact property deals).[31]

- Cross-Border Legal Knowledge: Given the international aspects of many scams, lawyers should familiarize themselves with treaties, foreign court procedures, and international evidence rules (like Hague Evidence Convention norms for electronic records).[32] Collaborative forums or continuing legal education programs can facilitate this learning.

- Strategic Litigation and Policy Advocacy: To close gaps, lawyers litigating on behalf of victims or public interest organizations should consider strategic litigation or policy advocacy initiatives, such as class-action litigation or public interest litigation. As an illustration, consumer attorneys could file motions in courts to rule that certain digital activities (such as automatic removal of fraud alerts without notification) be deemed against policy, triggering judicial instructions.

- Vetting Transactional Frameworks: Lawyers should demand face-to-face or video-verified settlements of even web-based transactions and propose multi-signature escrow systems (in which money is locked in multi-signed escrow by a neutral third party or program, pending fulfillment of specified terms). Legal units should explicitly address digital signatures and refer to court action in case of online fraud.

## Conclusion

The efficiency that the real estate sector has achieved through digital platforms has been matched by the sophisticated nature of fraudulent activities that exploit the same tools. We find that current Indian laws, including cyber laws and RERA, certainly offer protection but with significant gaps. Criminals and real estate fraudsters are taking advantage of lax identity

[31] See generally JERRY BRITO & PETER VAN VALKENBURGH, WRITING AND PUBLISHING ARTICLES ABOUT BITCOIN AND BLOCKCHAIN TECHNOLOGY: A STYLE GUIDE (2016).
[32] Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555.

verification and the slow pace of criminal prosecution. These scams have the potential to destroy public faith in online property markets if they remain unaddressed.

The solution requires finding a reasonable balance: rewrite laws (as demonstrated above), use technology (blockchain, AI) for prevention, and initiate collaboration between regulators, industry, and the legal community. Tighter regulation plus smarter platforms will help India enjoy the advantages of PropTech while protecting its realty industry against digital deception. Securing digital real estate transactions is as much a technical problem as it is a policy compatibility and enforcement challenge, and its success demands adaptive laws, creative solutions, and decisive cooperation.