ILE TAXATION LAW AND LEGAL STUDIES

VOLUME 3 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION

ILE TAXATION LAW AND LEGAL STUDIES

APIS – 3920 – 0024 | ISSN - 2583-9551

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://tlls.iledu.in/

Journal's Editorial Page - https://tlls.iledu.in/editorial-board/

Volume 3 and Issue 1 (Access Full Issue on - https://tlls.iledu.in/category/volume-3-and-issue-1-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

ILE TAXATION LAW AND LEGAL STUDIES

VOLUME 3 AND ISSUE 1 OF 2025

APIS – 3920 - 0024 *(and)* ISSN - 2583-9551 [IF SCORE – 7.58]

Published by

Institute of Legal Education

https://iledu.in

DEEPFAKE INVOICES & AI-GENERATED DOCUMENTATION FRAUDS: LEGAL READINESS OF INDIAN CUSTOMS

AUTHOR – FAIZ AKHTAR KHAN, STUDENT AT KIIT SCHOOL OF LAW, BHUBANESWAR, INDIA

BEST CITATION – FAIZ AKHTAR KHAN, WEAPONIZATION OF CUSTOMS DUTIES: THE US–CHINA TRADE WAR, *ILE TAXATION LAW AND LEGAL STUDIES (TLLS),* 3 (1) OF 2025, PG. 22-31, APIS – 3920 – 0024 & ISSN - 2583-9551

ABSTRACT

Artificial Intelligence is enabling the creation of highly realistic forged invoices and trade documents, posing fresh challenges for customs authorities. In India, existing laws – primarily the Customs Act, 1962; Information Technology Act, 2000; Indian Penal Code, 1860; and Evidence Act, 1872 – address fraud, forgery, and electronic evidence. However, these were not designed with AI-synthetic documents in mind. Current practice relies on risk-based profiling and post-hoc investigations (e.g., cases of forged export invoices). No prominent Indian case specifically involves "deepfake" invoices, although related cyberfraud incidents (like voice-cloned scams) have surged. This paper analyses the relevant legal provisions (Sections 114AA of the Customs Act; Sections 66C–66D of the IT Act; IPC Sections 463–471; Evidence Act Sections 65A–65B; etc.), notes enforcement gaps (e.g. needing digital-evidence certificates under Customs Act Section 139C), and recommends reforms. Suggestions include explicitly criminalizing AI-generated document forgery, adopting standardized forensic protocols (ISO/IEC 27037), enhancing international collaboration (WCO mutual assistance), and strengthening internal customs compliance and training for digital fraud detection.

Keywords: Artificial Intelligence (AI), Deepfake invoices, AI-generated trade documents, Customs fraud, Indian Customs, Customs Act 1962 (Section 114AA, Section 139C), Information Technology Act 2000 (Sections 66C–66D), Cyberfraud, Digital-forensics standards (ISO/IEC 27037), WCO mutual assistance

Introduction

AI-generated "deepfake" content has raised alarm internationally, with India observing a marked rise in AI-enabled scams and impersonations (voice-cloning, synthetic images, etc.)[61]. In trade facilitation, similar technology can produce entirely fabricated invoices or shipping documents that appear authentic. Such forgeries can be used to evade duties (by understating import values or falsely claiming exports) or launder money. Indian Customs relies heavily on documentation (invoices, bills of lading, shipping bills, etc.) to determine correct duty and compliance. This paper examines how the Indian legal framework addresses invoice/document fraud – particularly when AI is used – and whether Customs is prepared to counter the emerging threat of synthetic-document fraud.

We begin by surveying relevant Indian laws. We then review how Customs currently handles document-based fraud, including case examples of forged invoices or shipping bills. We assess gaps in the legal and regulatory regime – such as the absence of specific "deepfake" provisions and challenges in proving digital evidence authenticity – and conclude with recommendations to bolster preparedness

[61] https://indianexpress.com/article/technology/artificial-intelligence/ai-scams-surge-in-india-voice-cloning-deepfakes-and-otp-frauds-leave-victims-helpless-10232064/#:~:text=Story%20continues%20below%20this%20ad

ILE TAXATION LAW AND LEGAL STUDIES
VOLUME 3 AND ISSUE 1 OF 2025
APIS – 3920 - 0024 *(and)* ISSN - 2583-9551 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

(legislative amendments, forensic standards, international cooperation, and internal policies).

Legal Framework

1. Customs Act, 1962

The Customs Act, 1962 criminalizes false documentation and misdeclaration in import/export. Notably, **Section 114AA** makes it an offence knowingly to use a *false* or *incorrect* declaration or document to induce Customs to levy less duty. It prescribes a penalty up to five times the duty shortfall[62]. For example, if a deepfake invoice is used to under-declare import value, Section 114AA would apply. In addition, **Section 112** penalizes "improper importation" (dealing with goods liable to confiscation), and **Section 120** allows confiscation of goods fraudulently brought in. Customs investigation powers (Sections 110–113) enable seizure of goods, documents and examination of records[63]. In practice, Customs applies these provisions broadly to any attempt to defraud duties via documents.

Under customs rules, a recent tribunal decision emphasized that *digital* evidence must meet strict formalities. Section 139C (added by amendment) requires a certificate for secondary electronic evidence used in assessment. In *KDS Exports v. Commissioner of Customs* (CESTAT 2025), the tribunal set aside duty demands because data from an **unsealed computer** lacked the required Section 139C certification[64]. This effectively mirrors the general rule in Evidence Act Section 65B for electronic records: without a proper certificate, digital evidence may be inadmissible[6566]. Customs officers also follow guidelines (e.g., a 2024 CBIC instruction) that stress transparent, time-bound CI (commercial intelligence) investigations[67]. These ensure enquiries are specific and concluded within a year, indicating an emphasis on procedural rigor.

2. Information Technology Act, 2000

The IT Act provides for computer-related offences and legal recognition of electronic records. **Sections 43** and **66** address hacking, damaging computers and unauthorised access. In the context of forged invoices, **Section 66C** (punishing identity theft via electronic means) and **66D** (cheating by personation using computer) are pertinent. If an AI-generated document impersonates a legitimate trader or misuses someone's digital signature, these sections could apply (e.g., generating a bogus digital signatory certificate). The Act also grants *legal validity to electronic records and signatures* (Sections 4–5)[68]. This means electronic invoices and digital signatures are admissible, but wrongful creation can attract cybercrime penalties.

Notably, the Press Information Bureau notes that "the IT Act provides for punishment for offences considered as cybercrimes such as identity theft, cheating by personation, [etc.]". Thus, while there is no AI-specific offence, existing cyber-fraud provisions cover many deepfake abuses. However, proving intent and linking the synthetic nature of evidence to these offences may be challenging in practice.

3. Indian Penal Code, 1860

Traditional fraud and forgery offences in the IPC also apply. **Section 463–465** define and punish forgery, including of *"electronic record"* (per the IT Act amendment). For example, creating a

62 https://www.indiacode.nic.in/bitstream/123456789/15359/1/the_customs_act%2C_1962.pdf#:~:text=,following%20conveyances%20shall%20be%20liable

63 https://www.livelaw.in/tax-cases/customs-act-electronic-evidence-from-unsealed-cpu-without-any-s-139c-certificate-cannot-form-basis-of-assessment-cestat-309031#:~:text=Section%20139C%20certificate%20under%20the,form%20the%20basis%20of%20assessment

64 https://lawfinder.news/articles/Customs-Tribunal-Overturns-Duty-Demand-in-KDS-Exports-Case#:~:text=The%20Tribunal%20noted%20the%20absence,the%20assessment%2C%20based%20on%20contemporaneous

65 https://www.livelaw.in/tax-cases/customs-act-electronic-evidence-from-unsealed-cpu-without-any-s-139c-certificate-cannot-form-basis-of-assessment-cestat-309031#:~:text=Section%20139C%20certificate%20under%20the,form%20the%20basis%20of%20assessment

66 https://lawfinder.news/articles/Customs-Tribunal-Overturns-Duty-Demand-in-KDS-Exports-Case#:~:text=The%20Tribunal%20noted%20the%20absence,the%20assessment%2C%20based%20on%20contemporaneous

67 https://economictimes.indiatimes.com/news/economy/policy/cbic-asks-customs-officers-to-complete-inquiry-in-commercial-fraud-cases-within-a-year/articleshow/114976771.cms?from=mdr

68 https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2119050#:~:text=,any%20other%20technology%20and%20those

phony invoice or digitally altering an invoice would constitute forgery under Section 464, punishable under Section 465. Further, **Section 471** penalizes using a forged document as genuine. If an AI-generated invoice is submitted, Section 471 would cover its use. For cheating by deception, **Section 420** (cheating and dishonestly inducing delivery of property) may apply if a party is defrauded. Previous analyses note that deepfakes used to commit fraud can be charged as forgery under IPC §469[69]. Thus, even without AI-tailored laws, deepfake invoice fraud is not beyond the IPC: it falls under classic forgery and cheating provisions.

(Customs Act, 1962, §114AA)1; (Indian Penal Code, 1860, §§463–465, 468, 471)

4. Indian Evidence Act, 1872

Admissibility of electronic documents is governed by Sections **65A–65B**. Section 65A provides that electronic records satisfying certain conditions are admissible. Section 65B requires that any electronic evidence be accompanied by a **certificate of authenticity** (issued by the custodian) as a condition for admissibility. This was upheld in *Anvar P.V. v. P.K. Basheer* (2014) – the Supreme Court held that without a 65B(4) certificate, electronic evidence is inadmissible[70]. For Customs cases, a similar regime exists via Section 139C of the Customs Act (see above). Without compliance, crucial evidence (e.g. invoice data from a seized computer) may be excluded[71].

The Act also has presumptions for electronic agreements (Section 85A: digital signatures deemed genuine) and for output of computer (Section 85B). These presumptions aid prosecutions: an e-invoice with a valid DSC, for example, is presumed authentic. A deepfake invoice lacking proper digital signature would fail such presumptions. Overall, while electronic evidence is recognized, its procedural rigors (certificates, chain-of-custody) pose challenges if Customs officers are untrained in digital forensics or if standard operating procedures are not followed.

5. Other Relevant Laws

Several other statutes interface with invoice/document fraud:

- **Foreign Trade (Development & Regulation) Act, 1992:** Governs export-import policy. Violations (like fraudulent export claims) can attract penalties.
- **Foreign Exchange Management Act (FEMA), 1999:** Under-invoicing/over-invoicing implicates foreign exchange violations.
- **Prevention of Money Laundering Act (PMLA), 2002:** Large-scale customs fraud often triggers money-laundering probes. In the *Vikas Garg* case, the Enforcement Directorate invoked PMLA after CBI found massive fake export documentation[72].
- **Companies Act, 2013:** Punishes corporate officers if company falsifies records.
- **New Laws (2023–2024):** The Bharatiya Nyaya Sanhita (BNS) and Bharatiya Sakshya Adhiniyam (BSA) came into force mid-2024, updating IPC/Evidence. BNS retains forgery offences (see §§468–471 analogues) and BSA modernizes digital evidence (e.g. §85B requiring hash verification). These shifts are still unfolding and should be monitored.

In sum, India's legal framework lacks a standalone "deepfake" offence; such fraud must be squeezed into forgery/cheating and cybercrime statutes. The patchwork of laws does criminalize misleading official documents,

[69] https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world%3A-foreboding-and-forbidding#:~:text=,rooted%20restrictions%20in%20India

[70] https://www.indiacode.nic.in/show-data?actid=AC_CEN_3_20_00034_187201_1523268871700&orderno=71#:~:text=Section%2065B,Previous%20%20%2058

[71] https://lawfinder.news/articles/Customs-Tribunal-Overturns-Duty-Demand-in-KDS-Exports-Case#:~:text='The%20Tribunal%20noted%20the%20absence,the%20assessment%2C%20based%20on%20contemporaneous

[72] https://www.indiatoday.in/india/story/ed-raids-industrialist-vikas-garg-chairman-ebix-inc-others-rs-190-crore-customs-duty-fraud-case-2818452-2025-11-12

but enforcement has traditionally targeted analog forgery and conventional data. The rise of AI-generated documents thus exposes potential gaps in readiness.

Customs Enforcement and Fraud Cases

- **Risk Management and Compliance**

Indian Customs utilizes risk management systems (RMS) and audits to detect invoice fraud. RMS flags anomalous shipments (by value, origin, partner entities) for examination. A recent report indicated Customs reworked risk-profiles to tackle under-invoiced imports from China[73]. Investigators scan cargo data against historic norms and intelligence (e.g., unusually low invoice values prompt scrutiny). AEO (Authorized Economic Operator) programs encourage vetted importers to maintain valid documentation. Customs Commissioners may issue detailed notices for certain frauds and aim to wrap up "CI (commercial intelligence) cases" within a year[74]. Letters and summons in fraud probes now must specify the inquiry focus to ensure due process. These measures reflect an intent to balance enforcement with trade facilitation.

- **Investigative Agencies and Procedures**

On the ground, Customs frauds involving falsified docs often lead to multi-agency probes. The Directorate of Revenue Intelligence (DRI) and Central Bureau of Investigation (CBI) handle major commercial frauds, while the Central Board of Indirect Taxes and Customs (CBIC) guides policy. For example, in 2025, a joint CBI-ED operation cracked a network falsifying export records[75]. The ED (under PMLA) has impounded proceeds from such frauds (as in the Vikas Garg case)[76]. Customs laws allow seizure of contraband and documents (Sec 110), but pursuing documentary fraud often requires financial reconstruction. Banks and financial records are examined; Customs can share data with Income Tax and ED for a holistic probe.

Customs houses also empower officers to take statements (Section 108 of Customs Act) and compel record production. E.g., in *HBS Logistics v. Commissioner* (CESTAT 2024), a broker's employee admitted under Sec.108 that he submitted *forged examination documents* on orders of his principal[77][78]. This highlights internal controls: Customs routinely records confessions or witness statements under the Act. If a firm fails cooperation, licenses (like that of a customs broker) can be revoked.

- **Reported Incidents and Case Law**

While no public case explicitly names an "AI-generated invoice," many recent investigations involve sophisticated document forgery. In *HBS Logistics* (2024), a customs broker filed a Bill of Entry with fake first-page stamping (featuring non-existent officer signatures) to falsely indicate "no examination" was needed. The CESTAT upheld license revocation, underscoring that *fabricated* documents invalidated the clearance. Similarly, in an on-going DRI-CBI action, two businessmen (the Vikas Garg case) are accused of forging shipping bills and export invoices to pretend goods were exported to Nepal/Bangladesh, when they had been diverted domestically. Authorities estimated nearly ₹190 crore duty loss from this fraud. In these cases, conventional photocopy or manual forgery was used, but they illustrate the modus operandi: fake invoices *with real company names and customs seals*.

On the flip side, Customs has had technical victories: in late 2025, CESTAT Delhi rejected evidence from an **unsealed computer** lacking

[73] https://timesofindia.indiatimes.com/business/india-business/govt-probes-low-invoicing-of-imports-from-china/articleshow/97043910.cms#:~:text=The%20government%20has%20launched%20a,government%20officials%20said%20on%20Monday

[74] https://economictimes.indiatimes.com/news/economy/policy/cbic-asks-customs-officers-to-complete-inquiry-in-commercial-fraud-cases-within-a-year/articleshow/114976771.cms?from=mdr

[75] https://www.indiatoday.in/india/story/ed-raids-industrialist-vikas-garg-chairman-ebix-inc-others-rs-190-crore-customs-duty-fraud-case-2818452-2025-11-12

[76] https://www.freepressjournal.in/mumbai/ed-raids-industrialist-vikas-garg-others-in-190-crore-customs-duty-evasion-case#:~:text=The%20alleged%20fraud%2C%20officials%20said%2C,as%20exported%20to%20neighbouring%20countries

[77] https://www.legitquest.com/case/hbs-logistics-v-commissioner-of-customs/7A1523#:~:text=Smt,the%20importer%2C%20M%2Fs%20Supreme%20Enterprises

[78] https://www.legitquest.com/case/hbs-logistics-v-commissioner-of-customs/7A1523#:~:text=4,no%20further%20examination%20is%20required

the required Section 139C certificate[79]. In the *KDS Exports* (CESTAT 2025) appeal, imported flower valuations were challenged based on invoices "retrieved" from seized CPUs. The tribunal noted that absence of a 139C certificate and improper sealing meant the contested data could not override earlier bona fide assessments[80]. Thus, Customs law essentially mandates digital-evidence protocols, and failures (often by investigation teams) can derail prosecutions. The tribunal explicitly stressed that data without mandatory Section 139C certification "cannot form the basis of assessment".

While customs cases focus on quantifiable frauds, Indian courts have also begun addressing AI misuse in other contexts. The Supreme Court in *Anvar P.V. v. Basheer* (2014) laid down the need for 65B compliance for any electronic evidence in court – a rule that impacts customs adjudications too. More recently, high-profile Delhi HC actions (John Doe proceedings) have enjoined deepfake impersonation of celebrities[81]. These developments signal judicial awareness that synthetic media exist, but legislative attention remains general: deepfakes are dealt with as defamation or privacy breaches rather than as customs offences per se.

- **Customs and Digital Evidence**

As noted, Customs-specific rules (Sec.139C) require certificates like Evidence Act §65B. In practice, agencies have struggled with compliance. The *KDS Exports* tribunal and media reports reveal that DRI's computer forensic units must seal devices promptly and issue digital-certificates – or risk evidence being thrown out. In other words, Customs investigators must observe a strict chain-of-custody. The Evidence Act also presumes authenticity of proper digital signatures (Sec.85A), but if invoices arrive unsigned or with a phony signature, the presumptions fail.

To illustrate, consider an AI-generated PDF invoice. If the exporter has signed it with a valid digital certificate, Section 85A provides a rebuttable presumption that the signatory did it. An AI forgery without an actual private key signature would be prima facie fraudulent. But if criminals fabricate the signature itself (stealing a certificate), they could technically produce a document passing that presumption. Detecting such tampering requires technical forensics (checking certificate validity, cryptographic hash). Presently, Customs often lacks in-house cyber forensic capacity. In short, digital evidence rules are well-set but Customs must invest in ICT forensics to utilize them effectively.

- **Trends and Incidents**

Beyond cases, media and government reports highlight the broader landscape. The Press Information Bureau notes that Indian cyber laws (IT Act) and rules apply equally to AI-generated content[82]. Still, Customs anomalies continue. In 2023 the government publicly probed systematic low-invoicing of Chinese imports[83] – a form of under-reporting value to evade duty. This reflects that even without AI, invoice fraud is rampant. In GST regime (also under CBIC), "fake invoice" networks have emerged in the credit-chain. While GST fraud lies under indirect tax law, Customs faces analogous misuse (fake imports to claim duty drawbacks or refunds). For instance, media reported a ₹100+ crore GST refund scam based on bogus export bills (feds raided companies submitting exports of non-existent goods)[84]. Though not a customs case, it underscores the economy-wide risk of invoice fraud.

AI-specific scams have also hit India: recent press accounts document voice cloning and

[79] https://www.livelaw.in/tax-cases/customs-act-electronic-evidence-from-unsealed-cpu-without-any-s-139c-certificate-cannot-form-basis-of-assessment-cestat-309031?fromIpLogin=42695.079547627276

[80] https://lawfinder.news/articles/Customs-Tribunal-Overturns-Duty-Demand-in-KDS-Exports-Case#:~:text=The%20Tribunal%20noted%20the%20absence,the%20assessment%2C%20based%20on%20contemporaneous

[81] https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/#:~:text=2

[82] https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2119050#:~:text=,any%20other%20technology%20and%20those

[83] https://timesofindia.indiatimes.com/business/india-business/govt-probes-low-invoicing-of-imports-from-china/articleshow/97043910.cms#:~:text=The%20government%20has%20launched%20a,government%20officials%20said%20on%20Monday

[84] https://whitecollarprofessional.com/news-updates/685b76d68a25f9c00f63583c

deepfake video frauds where victims lost money[85]. These include "digital arrest" scams – imposters using AI to mimic cops or relatives. While such frauds are not trade-related, they demonstrate that synthetic media enable deception on a large scale. Customs should expect that savvy criminals might next "deepfake" official-looking trade docs. The legal system lacks reported incidents of pure "deepfake invoice" crime in India yet, but it is only a matter of time given global examples (e.g. Hong Kong executive losing $25.6 million in a deepfake CEO voice email scam). In anticipation, Indian law already permits prosecuting any resultant fraud under existing cyber and fraud statutes, even if the evidence medium is novel.

Regulatory and Enforcement Gaps

Despite broad coverage by existing laws, several gaps hinder effective action against AI-generated document fraud in customs:

- **Absence of AI-specific Statutes:** As one analysis notes, "deepfakes are not covered by any specific laws in India". The current law only addresses generic harms (defamation, privacy, cheating). There is no Customs Act provision explicitly criminalizing creation or use of synthetic trade documents. This means prosecutors must shoehorn cases into forgery or cheating, which may complicate proving the use of AI as a technique. A dedicated offence (or amendment) could explicitly encompass "any digitally generated or altered trade document" intended to mislead customs.
- **Digital Evidence Challenges:** Section 65B/139C formalities protect against tampered evidence but can hamper cases if not followed. Investigative lapses (unsealed devices, missing certificates) have nullified prosecutions. Many Customs field offices still lack standardized procedures for cyber-forensics. Further, AI-crafted invoices can defeat cursory checks (an on-screen copy may look genuine). There is no legal mandate requiring digital signatures on all high-value invoices, leaving a gap in verifiability. In short, digitization without corresponding forensic upgrades creates blind spots.
- **Technological Readiness:** Indian Customs has begun using data analytics and limited machine learning (e.g. for risk profiling)[86]. However, specialized tools to **detect manipulated documents or images** are generally absent. ISO/IEC standards (e.g. 27037 for digital evidence collection[87]) exist but are not yet ingrained in Customs labs. Without forensic watermarking or AI-detection software, deeply forged documents may slip through initial scrutiny. A similar gap is the use of blockchain or secure digital ledgers for trade documentation – such advanced protocols are not currently mandated for import/export papers in India.
- **Cross-border Enforcement:** Invoice fraud is often transnational. An under-invoiced import might involve collusion between an Indian importer and a foreign exporter or bank. Pursuing such cross-border fraud requires robust mutual legal assistance and intelligence-sharing. India has Customs Mutual Assistance agreements (e.g. with some Asian partners and via WCO frameworks), but the **practice** of exchanging information on suspicious invoices appears limited. For instance, a fake invoice generator in another

[85] https://indianexpress.com/article/technology/artificial-intelligence/ai-scams-surge-in-india-voice-cloning-deepfakes-and-otp-frauds-leave-victims-helpless-10232064/#:~:text=Story%20continues%20below%20this%20ad

[86] https://www.pwc.com/m1/en/publications/documents/2024/revolutionising-Customs-with-AI.pdf#:~:text=Indian%20customs%20developed%20an%20AI,making

[87] https://www.msab.com/updates/new-iso-standard-for-digital-evidence/#:~:text=New%20ISO%20standard%20for%20digital,identification%2C%20collection%2C%20acquisition%2C%20and

country could target Indian importers, and without an alert, Indian Customs may not detect the pattern. There is no mechanism to quickly flag an AI-doc generator to other jurisdictions. Also, multi-jurisdictional tracing of crypto-payments (if used) is a challenge.

- **Regulatory Coordination:** Indian Customs often works in silos from other regulators. While CBIC handles customs duties, the IT Ministry (MeitY) handles cyber governance. Coordination is improving (e.g. joint advisories on deepfake content), but trade-specific guidance on AI scams is lacking. For example, the IT Rules 2021 require social media to remove harmful deepfakes, but there is no equivalent mandate on industry platforms (like trade portals) to flag or label AI-generated commercial documents. Moreover, Customs intelligence may not routinely consult the National Cyber Crime Reporting Portal or CERT-In on emerging deepfake threats.
- **Internal Compliance and Awareness:** Many customs staff are well-trained in traditional smuggling and undervaluation, but may have limited exposure to AI-forensics. Regular training on cybersecurity and digital fraud is needed. On the trader side, importers/exporters might not be fully aware that presenting fraudulent digital documents can attract cybercrime penalties in addition to customs penalties. There is also a lack of internal compliance mandates for Customs Houses – unlike banks (which have KYC/AML rules), Customs has no equivalent "know your importer" obligation beyond the PAN/GST checks. This can allow shell companies to generate fake documents with impunity.

In summary, the Indian Customs framework treats deepfake-invoice fraud as fraud by other means. While theoretically prosecutable, in practice gaps in tech capability, inter-agency linkages, and specific legal clarity could be exploited by fraudsters.

Recommendations

To bolster Indian Customs against AI-generated document fraud, a multi-pronged strategy is needed:

Legal Reforms

- **Create an AI-Specific Offence:** Amend the Customs Act or IPC to define as an offence the creation or use of "synthetic or digitally manipulated trade documents" intended to deceive authorities. For example, a new subsection under Customs Act Chapter IV (Offences and Penalties) could parallel Section 114AA but explicitly mention AI tools or electronic falsification. Similarly, IT Act provisions could be updated: Section 66D (cheating by personation) might be broadened to cover impersonation via deepfake visuals, and a new section targeting "digital forgery" (akin to the proposed US "digital forgery" laws) could be introduced.
- **Evidence Act Updates:** The recently enacted **Bharatiya Sakshya Adhiniyam, 2023** should be leveraged. Its provisions (e.g. Section 85B) emphasize digital data integrity via hash and source certification[88]. Customs should promulgate rules aligning 139C with these standards. If not already done, issue secondary legislation requiring digital-certificate generation whenever a computer is seized. Also consider reversing or relaxing the Anvar strictures by allowing alternative proofs of authenticity (as some recent judgments suggest, e.g. *Arjun Panditrao* case). The

[88] https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/#:~:text=certificates%2C%20including%20hash%20and%20source,bolstering%20ethical%20and%20technological%20defences

key is to ensure evidence admissibility without letting procedural lapses let fraudsters off.

- **Harmonize Laws:** Ensure that "deepfake" falls under existing statutes. The Bharatiya Nyaya Sanhita (replacing IPC) contains updated cyber-crime chapters (Sections 336-356 on online forgeries) which could apply. Customs should educate its legal wings on invoking these provisions. Government could issue an official guideline clarifying that using AI to produce falsified customs documents constitutes forgery under §§468–471 of IPC (BNS equivalents). This would guide prosecutors and judges to interpret statutes broadly.
- **Regulate Digital Invoices:** Introduce mandatory digital signature or e-invoice standards for high-value imports. Under the GST regime, e-invoicing is mandatory above a turnover threshold; a similar approach could be adopted for customs. If importers must upload an e-invoice on ICEGATE signed by a registered e-invoice system, the chance of undetectable fake invoices shrinks. (Section 4 of IT Act already recognizes electronic records and signatures, so legality is clear; implementing rules can set secure digital protocols.)

Forensic and Technical Measures

- **Adopt International Standards:** Customs labs and investigation wings should follow ISO/IEC 17025 (testing competence) and ISO/IEC 27037 guidelines for digital evidence. Establish specialized cyber-forensic labs (or partner with agencies like CERT-In or NFSU) dedicated to customs cases. Provide accredited training to all investigating officers in collecting and preserving AI-manipulated evidence.
- **Deploy AI-Detection Tools:** Invest in software that can analyze documents for signs of forgery. Emerging tools (some research projects) can detect forged text, inconsistent fonts, or hidden artifacts. Customs could pilot such systems on risk-flagged invoices to pre-screen for anomalies before manual checks. Additionally, data analytics platforms (like Customs' "automated risk profiling") should incorporate red flags for duplicate or templated invoice content, unrealistic pricing patterns, or mismatches in commodity codes.
- **Digital Watermarking and Blockchain:** Explore technologies that secure trade documents. For example, encourage use of verifiable electronic seals or QR codes on invoices that can be checked against a database. The World Customs Organization (WCO) promotes "single window" and blockchain concepts for supply chain transparency. India might phase in voluntary registration of exporters in blockchain-based platforms, making invoice records tamper-evident.

Strengthening Enforcement and Cooperation

- **Interagency Task Forces:** Create permanent task forces on AI fraud involving Customs, DRI, CBI, ED, RBI, and CERT-In. This would institutionalize sharing of intelligence on suspicious cross-border transactions involving AI tools. For instance, if CERT-In notices deepfake campaigns targeting corporates, they could alert Customs that document fraud is emerging. Similarly, ED/Income Tax data on suspect wire transfers can be fed to Customs analytics.
- **International Collaboration:** Activate bilateral Customs Mutual Administrative Assistance (CMAA) agreements. Regular joint audits or data exchanges with major trading partners can uncover invoice laundering schemes. At the multilateral level, participate in WCO

initiatives on AI & blockchain in customs. Indian Customs officers should engage in global training programs (e.g., WCO capacity building) on trade-tech security. If cross-border criminals are identified (e.g., fake-export mills abroad), India should pursue MLATs and Interpol channels promptly.

- **Public-Private Partnerships:** Work with banks and fintechs. Given that payments often accompany invoices, partnering with RBI-regulated entities can catch patterns (e.g., incoming payments from shell importers). Encourage shipping lines and insurers to verify invoice authenticity when claims arise. Sharing anonymized fraud indicators with industry groups (like FIEO or CII) can raise red-flag awareness among legitimate traders.

Internal Policy and Training

- **Customs Staff Training:** Mandate regular cyber-fraud awareness workshops for Customs officers, including FIU training on e-investigations. Cases like HBS Logistics demonstrate that even procedural forgeries can be sophisticated; investigators must be alert to digital doc tampering. Create a "Digital Evidence Handbook" for Customs investigators, with checklists (e.g., seal CPUs upon seizure, obtain 65B certificates).
- **Guidance and Compliance:** Issue CBIC circulars on best practices. For example, a circular could require verification of the source of significant invoices (contact the exporter, cross-check PAN/GST). It might also direct that every impugned digital invoice be examined by a certified forensic examiner. Continue and expand programs like Authorized Economic Operator (AEO), rewarding importers with robust compliance systems (including internal audits of document authenticity).
- **Whistleblower Mechanisms:** Encourage insiders (e.g. bank officers, freight agents) to report suspicious invoice schemes, with confidentiality. Customs could partner with banks under CDD norms to flag irregular funding of imports from obscure companies.

Policy and Regulatory Measures

- **Intermediary Guidelines:** While IT Rules target online platforms, consider regulations for trade-related platforms. For instance, e-commerce marketplaces could be tasked (under trade law rules) to ensure vendors don't market goods with fraudulent origin docs. Though a niche area, it signals a regulatory ethos that digital commerce must be trustworthy.
- **Periodic Reviews:** Given rapidly evolving AI, establish a standing committee (perhaps under CBIC/MeitY) to review enforcement experiences and recommend updates. This body could include technologists, legal experts, and trade representatives. An annual report on "AI and Trade Fraud" could keep policymakers abreast.

Conclusion

Indian Customs faces a new frontier as AI makes document forgery cheaper and more convincing. The existing legal arsenal – Customs Act penalties, IPC forgery provisions, IT Act cyber offences, and Evidence Act requirements – can address many frauds, but they were not crafted with generative AI in mind. Enforcement practice likewise must evolve: recent tribunal rulings underline the importance of digital evidence procedure. To safeguard revenue and trade integrity, the law should catch up (e.g. by explicitly outlawing synthetic trade-document fraud) and Customs should enhance its techno-legal toolkit. Key steps include building forensic capabilities, tightening evidence protocols, and collaborating across borders and agencies. As one study on

deepfakes cautions, reliance on piecemeal application of general laws leaves gaps. A concerted Indian response – integrating legal reform with technical standards and institutional cooperation – will be needed to stay ahead of document-based AI fraud schemes.

Footnotes (Bluebook):

1. Customs Act, 1962, § 114AA.
2. Indian Penal Code, 1860, §§ 463–465, 468, 471.
3. Customs Act, 1962, § 139C.
4. IT Act, 2000, §§ 66C, 66D, 43.
5. Indian Evidence Act, 1872, §§ 65A–65B.
6. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
7. *HBS Logistics v. Commissioner of Customs*, CESTAT (Delhi), Customs Appeal No. 52249 of 2019 (Jan. 9, 2024).
8. *KDS Exports v. Commissioner of Customs (ICD), New Delhi*, CESTAT (Delhi), Customs Appeal (Principal) ___ of 2023 (Dec. 8, 2025).

References (APA):

Deshkar, A. (2025, September 7). *AI scams surge in India: Voice cloning, deepfakes and OTP frauds leave victims helpless*. Indian Express.

India Today. (2025, March 13). *Customs-ED nabs two businessmen for forging export documents*.

Times of India. (2023, Jan. 17). *Govt probes low invoicing of imports from China*.

MeitY (Ministry of Electronics & IT). (2025, April 4). *Government of India taking measures to tackle deepfakes* [Press release].

Panda, B. N. P., & Sharma, I. (2024). *Deepfake technology in India and world: Foreboding and forbidding*. Asian Institute of Research.

Free Press Journal. (2025, March 16). *Cbi, ED crack down on Rs 190-cr fake exporting case; two businessmen detained*.

Customs Officials/CBIC. (2024). *Commercial Intelligence (CI) case investigation guidelines*.