VOLUME XII FALL 2026 ISSUE 1

NLUJ LAW REVIEW

ISSN:2326-5320

12 (1) NLUJ Law Review

SEBI LODR REGULATIONS AND THE MISSING PIECE: WHY LISTED COMPANIES SHOULD DISCLOSE INSOLVENCY APPLICATIONS BY OPERATIONAL CREDITORS
Akshay Dhekane & Urvashi Singh

REGULATORY RESPONSES TO DEEPFAKES IN THE ELECTORAL PROCESS: A CONSTITUTIONAL AND STATUTORY EVALUATION UNDER INDIAN LAW
Charchit Pathak

COMPARATIVE ANALYSIS OF FRAUD PREVENTION IN RBI'S PAYMENT AGGREGATOR GUIDELINES AND THE EU'S PSD3 FRAMEWORK
Sumati Arora

FROM CONFLICT TO COHERENCE: REFORMING INDIA'S NETTING-INSOLVENCY INTERFACE
Soumya Jain & Nikhilesh Prajapati

REGULATING TOKENISED ASSETS: A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS, BANKING INTEGRATION, AND FUTURE POLICY DIRECTIONS
Harsh Mangalam

REFRAMING PN3: CLARIFYING BENEFICIAL OWNERSHIP AND REGULATORY OVERSIGHT IN INDIA'S LAND-BORDER FDI POLICY
Parth Gupta

THE DOMINO EFFECT OF BANK FAILURES: DO WE NEED A NEW SAFE HARBOUR INSOLVENCY PLAYBOOK?
Jagyansh Kumar & Sumit Patnaik

A NATIONAL LAW UNIVERSITY JODHPUR PUBLICATION

VOLUME 12 **FALL 2026** **ISSUE 1**

NLUJ LAW REVIEW

VOLUME 12 FALL 2026 ISSUE 1

NLUJ LAW REVIEW

SEBI LODR Regulations and the Missing Piece: Why Listed Companies Should Disclose Insolvency Applications by Operational Creditors.

Akshay Dhekane & Urvashi Singh 1

Regulatory Responses to Deepfakes in the Electoral Process: A Constitutional and Statutory Evaluation under Indian Law.

Charchit Pathak 38

Comparative Analysis of Fraud Prevention in RBI's Payment Aggregator Guidelines and the EU's PSD3 Framework.

Sumati Arora 76

From Conflict to Coherence: Reforming India's Netting-Insolvency Interface.

Soumya Jain & Nikhilesh Prajapati 104

Regulating Tokenised Assets: A Comparative Analysis of Legal Frameworks, Banking Integration, and Future Policy Directions.

Harsh Mangalam 142

Reframing PN3: Clarifying Beneficial Ownership and Regulatory Oversight in India's Land-Border FDI Policy

Parth Gupta 186

The Domino Effect of Bank Failures: Do We Need a New Safe Harbour Insolvency Playbook?

Jagyansh Kumar & Sumit Patnaik **219**

Akshay Dhekane & Urvashi Singh, *SEBI LODR Regulations and the Missing Piece: Why Listed Companies Should Disclose Insolvency Applications by Operational Creditors,* 12(1) NLUJ L. Rev. 1 (2026)

SEBI LODR REGULATIONS AND THE MISSING PIECE: WHY LISTED COMPANIES SHOULD DISCLOSE INSOLVENCY APPLICATIONS BY OPERATIONAL CREDITORS

~Akshay Dhekane & Urvashi Singh[*]

ABSTRACT

Disclosure requirements are an essential aspect of SEBI's regime of market regulation, fostering transparency and enabling investors to make informed decisions. Lack of adequate disclosures can conceal actual risks and a company's true financial health. This is particularly concerning when a company faces insolvency. Despite this, the current regulatory framework under the LODR Regulations, fails to require the disclosure of insolvency applications filed by operational creditors under the IBC.

Through this paper we examine this regulatory gap and argue that the qualitative and quantitative significance of filing of these insolvency applications require their disclosure. Initiating a CIRP, irrespective of the creditor type constitutes a material event that requires timely and adequate disclosure. Through an examination of the LODR Regulations and SEBI's Adjudication Orders, we explore SEBI's de facto approach towards disclosing these insolvency filings, which, whether directly or indirectly, mandates their disclosure.

[*] Akshay Dhekane is a lawyer based in Mumbai and holds a B.A. LL.B. (Hons.) from National Law University Delhi and Urvashi Singh is a lawyer based in Mumbai and holds a B.A. LL.B. (Hons.) from National Law University Delhi.

We argue that this requirement should be formalized to ensure regulatory consistencies, protect investors and preserve market integrity. Considering insolvency applications as a deemed material event, a case has been made for aligning the disclosure requirement with the SEBI's broader objectives.

TABLE OF CONTENTS

I. INTRODUCTION 4

II. THE REGIME OF DISCLOSURE FOR INSOLVENCY EVENTS 7

A. OPERATIONAL CREDITORS INITIATING CIRP AND THEIR DISCLOSURE REQUIREMENTS UNDER LODR REGULATIONS 7

B. DIFFERENTIAL TREATMENT OF CREDITORS UNDER THE IBC AND SEBI LODR REGULATIONS..... 13

I. SECTION 9 INSOLVENCY APPLICATION AS A 'MATERIAL EVENT' UNDER LODR REGULATIONS..... 18

A. UNDERSTANDING DISCLOSURE REQUIREMENTS UNDER LODR REGULATIONS 19

B. DISCLOSURES UNDER PARA A – DEEMED MATERIAL EVENTS 20

C. DISCLOSURES UNDER PARA B – APPLYING MATERIALITY GUIDELINES 23

II. SECTION 9 APPLICATION AS A 'MATERIAL EVENT': AN ANALYSIS OF PRECEDENTS..... 31

A. THE PRECEDENTS 31

III. CONCLUSION.....35

I. INTRODUCTION

The securities market is a vital source for companies to source capital from the public, making it an important component of economic growth.[1] With a strong legal and regulatory framework, the securities markets promote investor welfare[2] which is critical for long-term economic development. This is supported by the fact that disclosure requirements are an important aspect of Securities and Exchange Board of India's ("**SEBI**") regulation of capital markets.[3] To that end, SEBI has imposed stringent disclosure standards to improve market transparency and investor safety through the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("**LODR Regulations**").

LODR regulations require listed companies to provide detailed disclosures about a variety of topics, including financial performance, corporate governance procedures, and major developments. These requirements bring transparency, enabling investors, market participants, and creditors to assess a company's financial position,[4] while also increasing confidence about markets being fair.[5] They preserve the integrity and

---

[1] RAYMOND W. GOLDSMITH, FINANCIAL STRUCTURE AND DEVELOPMENT 114,115 (Yale University Press 1959).

[2] Carol J. Simon, '*The Effect of the 1933 Securities Act on Investor Information and the Performance of New Issues*' 79(3) THE AMERICAN ECON. REV. 295 (1989).

[3] G. Sabarinathan, '*Securities and Exchange Board of India and the Regulation of the Indian Securities Market'* IIM BANGALORE RESEARCH PAPER NO. 309 20(May 07 2024) https://www.iimb.ac.in/sites/default/files/2018-07/WP_No._309.pdf.

[4] *In the matter of Citizen Yarns Limited,* SEBI Adjudication Order Ref No.: EAD-2/SS/VS/2018-19/2168.

[5] Varun Mansinghka & Kastubh Madhavan, *'Disclosure Obligations of Listed Companies in India: The Past, the Present and the Future*' INT'L BUS. L.J. 323 (2016).

openness in the financial markets and allow the regulators to supervise corporate actions. The Securities Appellate Tribunal ("**SAT**") emphasized that timely and accurate disclosures fulfil two essential functions.[6] *Firstly*, they enable investors to make an informed decision regarding which scrips to invest in. *Second*, SEBI can properly monitor the transactions in the capital markets to effectively regulate them. In addition, the disclosure requirements bring about transparency in the transactions in the market.[7]

However, certain complex disclosures fail to accurately highlight the actual risks involved and the real fundamentals of the company.[8] For instance, a company may strictly interpret the law to reduce its compliance and avoid accountability brought by disclosures. This lack of transparency becomes particularly concerning when a company faces financial distress, which has the potential to culminate in insolvency.[9] An often-overlooked area within this context is disclosure requirements involving operational debts. This paper highlights this key regulatory gap: the absence of a disclosure requirement under the LODR Regulations for listed companies when an operational creditor files an insolvency application against them.

---

[6] Coimbatore Flavors & Fragrances Ltd. & Ors v. SEBI, Appeal No. 209 of 2014 (August 11, 2014).
[7] Milan Mahendra Securities Pvt. Ltd. v. SEBI, Appeal No.66 of 2003 order dated April 15, 2005.
[8] Benjamin Fung, *The Demand and Need for Transparency and Disclosure in Corporate Governance* 2(2) UNIVERSAL J. MGMT. UNIVERSAL JOURNAL OF MANAGEMENT 72, 74. (2014).
[9] Harlan Platt & Marjorie Platt, *Understanding Differences between Financial Distress and Bankruptcy* 2(2) REV. APPLIED ECON. 141. (2006).

Initiation of CIRP under Section 9 of the IBC represents a serious default with serious consequences. The minimum threshold for an operational creditor to file such an application is □ 1 crore, which must be independently satisfied, thus underscoring the significance of the underlying claim.[10] These applications can trigger a moratorium, transfer of management control, and even liquidation, regardless of the company's formal financial position. They have a material impact on shareholder value, creditworthiness, and investor confidence, and they raise questions about a company's governance and its capacity towards creditors' obligations. Thus, the absence of a clear regulatory requirement for listed companies to disclose such applications creates a concerning gap. It risks distorting market transparency and investor decision-making.

Thus, this paper addresses this regulatory ambiguity by evaluating whether filings under S.9 of the IBC should be considered material events under the LODR Regulations, and argues in favour of a consistent and predictable disclosure framework. It examines the breadth and implementation of disclosure requirements of a material event, i.e., the filing of insolvency applications by operational creditors. Part II examines the insolvency regime and its incorporation in the LODR Regulations through the 2018 Amendment. Part III focuses on Schedule III of the LODR Regulations, highlighting the reasons which may require a listed company to disclose the filing of an application by an operational creditor

[10] Megha Mittal & Shreya Jain, *IBC Threshold Raised: Analysis and Implications*, INDIACORPLAW 28 March 2020, https://indiacorplaw.in/2020/03/28/ibc-threshold-raised-analysis-and-implications/ .

for the initiation of CIRP against the corporate debtor. Finally, Part IV concentrates on the precedents that establish the obligation for a listed company to report the filing of an application by an operational creditor. We analyse two judicial precedents, followed by a practical example illustrating a listed company's compliance with this requirement.

II. THE REGIME OF DISCLOSURE FOR INSOLVENCY EVENTS

This section explores the insolvency regime under the Insolvency and Bankruptcy Code, 2016 ("**IBC**" or "**the Code**"), particularly from an operational creditor's ("**OC**") perspective. It analyses the evolution of the regulatory framework governing disclosure requirements involving operational creditors and highlights the differential treatment they face under the current law. Finally, it evaluates the rationale behind this distinction.

A. OPERATIONAL CREDITORS INITIATING CIRP AND THEIR DISCLOSURE REQUIREMENTS UNDER LODR REGULATIONS

The Corporate Insolvency Resolution Process ("**CIRP**") aims at insolvency resolution in a way that maximises the value of the assets and promotes entrepreneurship. The IBC *primarily* deals with two types of creditors – financial and operational creditors, and both of them can initiate CIRP. A financial creditor is an individual or entity to whom a financial

debt is owed, and includes those who have acquired the debt through assignment or transfer.[11]

The term "*financial debt*" is defined under S.5(8) of the IBC, encompassing loans, debentures, guarantees, and "amounts raised under any other transaction, including any forward sale or purchase agreement, having the commercial effect of a borrowing. On the other hand, an operational creditor, as defined by S.5(20) of the IBC, is any individual or company who is legally owed operational debt, as well as those to whom such obligation has been lawfully assigned or transferred.[12] Operational debt means a claim pertaining to the trade of products or services. It also covers debts owed to employees or to the Central or State Government or any other body for the repayment of debts originating under any legislation.

S.9 of the IBC allows an operational creditor to file an application for initiating a CIRP against a corporate debtor, i.e., it is a pre-CIRP event. For initiating CIRP, S8 lays down certain pre-conditions.[13] The Supreme Court of India ("**Supreme Court**") in *Mobilox Innovations (P) Ltd. v. Kirusa Software (P) Ltd.*[14] articulated the requirements of ss. 8 & 9 of the Code in three steps:

i. Default must have taken place.

---

[11] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 5(7) (India).
[12] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 5(20) (India).
[13] Next Education India (P) Ltd. v. K12 Techno Services, (2023) 238 Comp Cas 101.
[14] Mobilox Innovations Private Limited v. Kirusa Software Private Limited, Supreme Court, 2018 (1) SCC 353.

ii. A demand notice requesting payment for an outstanding operational debt must be sent.
iii. The debtor either fails to respond within ten days of receiving the demand notice, or their response adduces no repayment or a pre-existing dispute.

Thus, an operational creditor is required to send a demand notice to the debtor on their default, to which the debtor must reply within ten days. They may dispute this demand notice or provide proof of repayment of dues. If the debtor does not respond to this demand within this timeframe, the operational creditor has the right to initiate CIRP against the debtor. Typically, this insolvency process is categorised into three different stages[15]:

1. Pre-CIRP period, which is the time period before the application is accepted by the Adjudicating Authority ("**AA**").
2. The CIRP period, which lasts from the National Company Law Tribunal accepting the application until the resolution plan is approved by the AA.
3. Post-CIRP period, which refers to the period during which the resolution plan approved by the AA is being implemented.

[15] Neeti Shikha and Urvashi Shahi, Assessment of Corporate Insolvency and Resolution Timeline (Insolvency and Bankruptcy Board of India 2021) RP-01/2021 , https://ibbi.gov.in/uploads/publication/2021-02-12-154823-p3xwo-8b78d9548a60a756e4c71d49368def03.pdf

The Insolvency and Bankruptcy Board of India ("**IBBI**"), through a circular[16] emphasised that a company must abide by all the applicable laws during various insolvency proceedings. In India, a listed company is required to make disclosures as per the LODR Regulations.[17] The basis for outlining the rules guiding listed companies' disclosure obligations can be identified in Regulation 4 of Chapter II of the LODR Regulations 2015. Regulation 4 underscores the necessity of transparency and prompt information sharing with investors and stock exchanges. Thus, if a listed company is undergoing a CIRP, it must generally comply with the LODR Regulations. However, in March 2018, SEBI, in its consultation paper on '*Compliance with SEBI Regulations by listed entities undergoing CIRP under the IBC*'[18] ("**CIRP Discussion Paper**") identified that there were no specific disclosure requirements pertaining to pre-CIRP or the CIRP stage in the LODR Regulations.

Thus, noting this gap, SEBI proposed certain amendments to Regulation 30 of the LODR Regulations in 2018.[19] These amendments proposed mandatory disclosure requirements for the following events to the stock exchanges. *Firstly*, the filing of an insolvency application for the

---

[16] Insolvency and Bankruptcy Board of India, '*Insolvency professional to ensure compliance with provisions of the applicable laws*' circular dated January 03, 2018 No. IP/002/2018, https://ibbi.gov.in/webadmin/pdf/whatsnew/2018/Jan/CIRP%202_2018-01-03%2018:41:44.pdf.

[17] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015.

[18] SEBI Discussion Paper, *Compliance with SEBI Regulations by listed entities undergoing Corporate Insolvency Resolution Process under the insolvency and bankruptcy code* , 2016 (28 March 2018), https://www.sebi.gov.in/sebi_data/commondocs/mar-2018/Discussionpaper10_p.pdf. ("**CIRP Discussion Paper**")

[19] *Id.*

initiation of CIRP by the corporate applicant. *Secondly*, the filing of an insolvency application by the creditors against the corporate debtor for the initiation of CIRP. *Thirdly*, disclosing the amount in default, as outlined in applications submitted by the creditors or by the corporate applicant to the NCLT. *Fourthly*, listed corporate debtors were to disclose the receipt of demand notices or invoices demanding payment of defaulted amounts from operational creditors, in accordance with S.8(1) of the IBC. *Finally*, the admission of applications by the NCLT.

This proposed amendment aimed to make it mandatory for listed companies undergoing CIRP to disclose at various stages the progress that was being made under the CIRP. Notably, in this proposal, SEBI did not differentiate between the creditors filing a CIRP application and also required disclosure of a demand notice from an operational creditor. However, when the LODR Regulations were actually amended[20] two key disclosures regarding operational creditors were omitted.[21] The first omission was the obligation to report the receipt of demand notices or invoices. The second was the requirement to disclose the filing of an application under S.9 of the IBC. Therefore, when the Amendment came into effect, the filing of an insolvency application by an operational creditor was not required to be disclosed, whereas applications filed by financial

[20] SEBI (Listing Obligations and Disclosure Requirements) (Third Amendment) Regulations 2018.
[21] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Schedule III Part A Para A, Clause 16.

creditors and by the corporate applicant themselves were still subject to disclosure.[22]

Disclosure of the filing of S.9 applications remains essential for two key reasons. *First*, under the IBC, a corporate debtor has the opportunity to either pay or dispute the demand notice issued by an operational creditor. It is only upon the debtor's failure to respond that the operational creditor may initiate CIRP. This mechanism indicates that the debtor had notice of the default and failed to rectify it, which can have dire implications for stakeholders. *Second*, the law prescribes a fourteen-day timeline for the AAs to decide on the admission of such applications; this deadline is considered "*procedural and directory*"[23] and is rarely adhered to. The Standing Committee on Finance identified the admission stage of CIRP applications as a key stage where most delays occur.[24] According to data from the IBBI, not a single Section 9 application was admitted within 14 days during 2020 – 2021 and 2021 – 2022; and the average time to admission was 468 days and 650 days, respectively, in those years.[25] Such prolonged delays generate significant information asymmetry in the market, depriving investors of

[22] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Schedule III Part A Para A, Clauses 16(a) and 16(b).
[23] Surendra Trading Company v. Juggilal Kamlapat Jute Mills Co. Ltd. & Ors, NCLAT Delhi Company Appeal (AT) (Insolvency) No. 189 of 2018 (43).
[24] Ministry of Corporate Affairs Standing Committee on Finance, *Implementation of Insolvency and Bankruptcy Code- Pitfalls and Solutions* (Thirty-Second Report 2020-2021).
[25] Insolvency and Bankruptcy Board of India, *Consultation paper on issues related to reducing delays in the corporate insolvency resolution process* (April 13, 2022), https://ibbi.gov.in/uploads/whatsnew/72a560ce5697bbaeef62ce5893a3f1ad.pdf.

timely insights into the company's governance, debt servicing capacity and solvency.

These observations focus towards the broader issue of differential treatment between financial and operational creditors,[26] and calls for a brief examination of the regulatory rationale for such a distinction under the LODR Regulations.

B. DIFFERENTIAL TREATMENT OF CREDITORS UNDER THE IBC AND SEBI LODR REGULATIONS

IBBI treats financial and operational creditors differently in three key aspects. *First*, operational creditors are excluded from the Committee of Creditors ("**CoC**"), which determines the approval or rejection of insolvency resolution plans, if financial creditors are present in the CoC.[27] Although operational creditors with at least 10% of the debtor's outstanding debt can attend CoC meetings, they do not have any voting rights.[28] *Second*, financial creditors are given a priority over operational creditors in the distribution of liquidation assets as per the waterfall mechanism under S. 53 of the IBC. This distinction is often criticised as both creditor types are contractually equal, and prioritising one over the

---

[26] C. Scott Pryor and Risham Garg, '*Differential Treatment Among Creditors Under India's Insolvency and Bankruptcy Code, 2016: Issues and Solutions*' (2020) 94 American Bankruptcy Law Journal 123, 141-143.

[27] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 21(2) (India).

[28] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, §§ 24(3)(c) and 24(4) (India).

other may conflict with principles of natural justice.[29] *Third*, financial creditors can initiate CIRP upon default without specific requirements, whereas operational creditors must fulfil certain conditions under ss. 8 and 9 of the IBC, as highlighted above, reflect procedural inequity.

The Bankruptcy Law Reforms Committee ("**BLRC**"), in their report, provided the rationale behind the differential treatment of the creditors in the CoC by stating that only financial creditors have the capability to assess the viability of the debtor and the willingness to negotiate terms of existing liabilities. They noted that operational creditors are typically not equipped to make decisions or assume risk in the debtor's business.[30] The Supreme Court in *Swiss Ribbons Pvt. Ltd. & Anr. v. Union Of India & Ors* ("**Swiss Ribbons**")[31] held that the preferential treatment of financial creditors under the S.53 of the IBC does not violate Article 14 of the Indian Constitution, which guarantees protection against discrimination. Primarily relying on the BLRC, the Court upheld the distinction between the operational and financial creditors in the waterfall mechanism[32] and the process for initiating insolvency proceedings.[33] The Court held that there is an intelligible differentia between the two creditors, considering their business relations with the corporate debtor, thus

---

[29] R Shankar Raman, *Moving towards Improved Rights of Operational Creditors under the IBC- An Analysis in IBC: Evolution, Learnings and Innovation* 20 (Insolvency and Bankruptcy Board of India, 2023).

[30] REPORT OF THE BANKRUPTCY LAW REFORMS COMMITTEE, Vol. 1, under Para 5.3.1, sub-para. 4 on p. 84 November, 2015.

[31] Swiss Ribbons Pvt. Ltd. & Anr. v. Union Of India & Ors (2019) 3 S.C.R. 535.

[32] *Id.* ¶28.

[33] *Id.* ¶38.

justifying that this distinction is not discriminatory.[34] However, this understanding is often criticised for being inherently unfair, lacking a strong rationale, and failing to adequately protect the interests of operational creditors.[35] Furthermore, recent judicial and legislative trends indicate a shift towards equitable treatment of operational creditors. In *Binani Industries v. Bank of Baroda*[36] the NCLAT ruled that resolution plans cannot discriminate between similarly situated financial and operational creditors without valid justification, reinforcing the principle of fairness and non-discrimination. Further, the amended Regulation 38(1) of the IBBI (Insolvency Resolution Process for Corporate Persons) now mandates that operational creditors are given priority over financial creditors in the distribution of amounts under a resolution plan. This Regulation, when read alongside S. 30(2)(b) of the IBC, which requires that operational creditors must receive at least the liquidation value they would be entitled to under S. 53, reinforces the statutory intent to provide equitable treatment. Lastly,

---

[34] See, Committee of Creditors of Essar Steel India Limited (through authorized signatory) v. Satish Kumar Gupta and Others, (2020) 8 SCC 531.

[35] Sudip Mahapatra, Pooja Singhania and Misha Chandna, '*Operational Creditors in Insolvency: A Tale of Disenfranchisement*' (*S&R Associates* 30 July 2020), https://www.snrlaw.in/operational-creditors-in-insolvency-a-tale-of-disenfranchisement ; Vinod Kothari & Sikha Bansal, *Subordination of Operational Creditors under IBC: Whether Equitable*? (INDIACORPLAW 23 July 2018), https://indiacorplaw.in/2018/07/subordination-operational-creditors-ibc-whether-equitable.html.

[36] *Binani Industries v. Bank of Baroda*, Company Appeal(AT) (Insolvency) No. 82 of 2018 (23).

even the Report of the Insolvency Law Committee (February 2020) highlighted that "*operational creditors may be conferred voting rights in the future*".

While the arguments for differential treatment of financial and operational creditors under the IBC may hold, there is no justification for such regulatory distinctions for making disclosures under the LODR Regulations. SEBI's mandate revolves around investor protection and regulating the securities market[37] and is fundamentally different from the IBC. By excluding operational creditors from pre-CIRP disclosures, SEBI risks undermining its own objectives. Besides, there has not been any guidance note or any literature from SEBI on this, which clarifies their rationale for making this distinction between these creditors.

An argument against mandating mandatory disclosures for operational creditors might be based on the differential treatment rationale in *Swiss Ribbons*. This argument suggests that operational debts are smaller in amount, often recurring, and are more likely to be disputed compared to financial debts.[38] Hence, disclosing S. 9 IBC filings might flood the market with excessive information.

However, this argument does not hold for two reasons. *First*, presumably, the reason for the exclusion of disclosure requirements relating to the filing of insolvency applications by operational creditors may lie in the low default threshold that existed prior to 24 March 2020. At that time, the threshold for initiating CIRP was set at □1 lakh, which may have

[37] SEBI Act, 1992, Preamble No. 15, Acts of Parliament, 1992 (India).
[38] *Supra* note 31, ¶50.

allowed CIRP to be triggered by operational debts of relatively insignificant value, potentially leading to insolvency or liquidation of a company on minor defaults. However, with a subsequent notification, the threshold for the minimum default amount was revised to □ 1 crore.[39] Thus, any claim made by an operational creditor now necessarily involves a substantial financial stake. Furthermore, as per the explanation to S.7 of the IBC, a significant disparity exists between financial and operational creditors in meeting the default threshold for initiating CIRP. corporate insolvency resolution. While financial creditors are permitted to aggregate defaults across multiple creditors to satisfy the □ 1 crore threshold, operational creditors are not allowed such flexibility.[40] An operational creditor must independently establish that the defaulted amount owed to them alone meets the prescribed threshold. The claim of one operational creditor cannot be clubbed with those of others, thereby creating a higher entry barrier for operational creditors seeking to initiate insolvency proceedings under the IBC. Hence, given that the IBC prescribes a stringent and structured process for operational creditors to initiate CIRP, it is difficult to justify SEBI's omission of corresponding disclosure requirements.

Second, as SEBI's regulatory framework already requires all material events to be disclosed, and an insolvency application, irrespective of the

---

[39] Ministry of Corporate Affairs, Notification No. S.O. 1205(E), Gazette of India, 24 March, 2020.

[40] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 7 (India); See Innoventive Industries Ltd. v. ICICI Bank and Anr Civil Appeal Nos. 8337-8338 of 2017 (28).

creditor's nature, is undeniably material (*discussed in detail below in Chapter III*). Moreover, initiating CIRP signals potential financial instability within the company. It signifies a threat to the existence of the company, as it is a real possibility that a corporate debtor may be liquidated at the end of the CIRP.[41] Disclosing this information will ensure transparency, boost investor confidence, and provide an accurate representation of the company's financial health.

Thus, it is important to examine whether operational creditors' filing of an insolvency application under S. 9 would amount to a material event. This requires a detailed interpretation of the existing legal framework governing such disclosures and how they are to be read with the LODR Regulations.

I. SECTION 9 INSOLVENCY APPLICATION AS A 'MATERIAL EVENT' UNDER LODR REGULATIONS

This section examines provisions of the LODR Regulations concerning the filing of insolvency applications by operational creditors against listed entities. It examines SEBI's treatment of disclosure requirements of operational creditor-initiated insolvency applications through these Regulations.

While the LODR Regulations do not explicitly mandate the disclosure of applications filed under Section 9 of the IBC, a contextual

[41] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 54(1) (India); Insolvency and Bankruptcy Board of India (Liquidation Process) Regulations, 2016.

interpretation of various entries suggests that listed companies are nonetheless required to disclose such filings, thereby creating an indirect disclosure obligation requirement. To substantiate this, the first part examines the mandatory disclosure requirements under the LODR Regulations. It then focuses on non-mandatory disclosures, specifically those related to pending litigation via application of quantitative thresholds. Taking these together, it is argued that operational creditor applications under s.9 of the IBC should be disclosed, even in the absence of an explicit regulatory obligation.

A. UNDERSTANDING DISCLOSURE REQUIREMENTS UNDER LODR REGULATIONS

Regulation 30 of the LODR Regulations deals with the "*Disclosure of events and information*". It provides that every listed entity shall make disclosures of any events or information which are material in the opinion of the board of directors of the listed company.[42] That said, determining what constitutes a 'material event' is inherently difficult and lacks a defined definition, despite its widespread use in legislation, rules, and regulations. To address this, Part A of Schedule III of LODR Regulations lists events/information which can be considered material for listed companies. Part A is categorised into:

[42] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Regulation 30(1).

1. Para A events/information – These events/information are deemed material. These have to be mandatorily reported to the stock exchanges without being subjected to any test of materiality.[43]
2. Para B events/information – These events/information are subject to the materiality guidelines under Regulation 30(4) and are to be reported to the stock exchanges if any of the specified criteria are met.[44]

Failure to disclose events/information as per the LODR Regulations leads to imposition of fines; suspension of trading; freezing of promoter/promoter group holding of designated securities, and any other action as may be specified by the Board from time to time.[45] The SEBI Act prescribes a penalty of a maximum amount of one crore rupees for failure to comply with these Regulations.[46]

B. DISCLOSURES UNDER PARA A – DEEMED MATERIAL EVENTS

Para A events are inherently material and there under Clause 6 provides that a listed entity must disclose 'defaults or frauds' by a listed company, or its management. LODR Regulations define default as "*non-payment of the interest or principal amount in full on the date when the debt has become*

[43] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Schedule III Part A Para A.
[44] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Regulation 30(4).
[45] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Regulation 98.
[46] SEBI Act, 1992 s. 15A(b) No. 15, Acts of Parliament, 1992 (India).

due and payable".[47] On the other hand, the IBC defines default[48] as non-payment of debt when the corporate debtor fails to repay the entire amount owed, in part, or in instalments after the debt has become due and payable. These two definitions overlap, focusing on the failure to fulfil financial obligations, regarding debt repayment. However, unlike the IBC,[49] The LODR Regulations do not distinguish between financial and operational creditors when defining a default.

Further, the term 'debt' is not defined under LODR, while under the IBC, debt means, "*a liability or obligation in respect of a claim which is due from any person and includes a financial debt and operational debt*."[50] Clause no 6 does not specify the kind of creditor (whether financial or operational) towards whom the corporate entity is in default.[51] This forms a legal position that a listed company must mandatorily disclose defaults towards *all* its creditors to the stock exchanges.

Apart from facilitating insolvency resolution, the purpose of introducing pre-CIRP disclosure was to ensure protection of investors' interests in the securities markets.[52] An insolvency application, regardless of

---

[47] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Schedule III Para A Part A, Clause 6(ii).
[48] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 3(12) (India).
[49] Global Credit Capital Limited & Anr. v Sach Marketing Pvt. Ltd. & Anr, 2024 INSC 340.
[50] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 3(11) (India).
[51] *Supra* note 50.
[52] SEBI, CIRP Discussion Paper (n 18); *Supra* note 18 1.

whether it was initiated by operational or financial creditors, possibly signifies a threat to the existence of the company, as it remains a possibility that the corporate debtor undergoes liquidation.[53] It is a qualitative material event, and it reflects on the quality of corporate management practices.[54] Some authors argue that even allegations of default, which could potentially lead to insolvency, are considered serious and must be disclosed.[55]

LODR Regulations provide for a mandatory disclosure of a default, but are silent on an operational creditor's insolvency application, which is a more severe event for a company. The corporate debtor can respond to a demand notice by either making payment or notifying of a pre-existing dispute in its relation. Thus, the corporate debtor's failure to respond in either manner strengthens the possible admittance of the operational creditor's insolvency application.[56] This inaction by the debtor suggests a potential inability to meet financial obligations, which can lead to CIRP. Additionally, the inability to pay operational creditors who are often suppliers, employees, or government authorities, may indicate cash flow issues in the company. Operational debts are typically smaller in quantum, and a failure to pay can highlight that liquidity issues have escalated to the point where even basic obligations are not met. Therefore, it is reasonable

---

[53] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 54(1) (India); Insolvency and Bankruptcy Board of India (Liquidation Process) Regulations, 2016.

[54] Michael G. Michaelson, '*Breach of Trust: The Duty to Disclose Pending Litigations in a Contest for Corporate Control*' 37 RUTGERS L. REV. 1, (1984).

[55] *Id.*

[56] In the matter of insider trading activities in the scrip of Shilpi Cable Technologies Ltd, SEBI Adjudication Order Ref No: /GR/HK/2023-24/28062-28064 (32).

to infer that the company can be at a higher risk of defaulting on more substantial, long-term financial debts.

Lastly, the LODR Regulations does not provide any monetary threshold of default that must be reached to warrant disclosure.[57] The absence of a monetary threshold for the disclosure of default means that all listed companies would be required to disclose any defaults that they make on an operational debt, regardless of its quantum or frequency.

C. DISCLOSURES UNDER PARA B – APPLYING MATERIALITY GUIDELINES

This section demonstrates that the filing of an insolvency application by an operational creditor qualifies as a material event under Regulation 30(4) of the LODR Regulations. Although these filings are not specifically covered, it is argued that they should be disclosed mandatorily. Reliance is placed on a comprehensive reading of the LODR Regulations, particularly on a Para B event, which requires disclosure of pending litigations. This is supported by the application of the materiality criteria under the Regulations.

Clause 8 of Para B of Part A of Schedule III provides that the "*pendency of any litigation(s) or dispute(s), or the outcome thereof which may have an impact on the listed entity*," shall be disclosed upon applying materiality criteria

[57] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Schedule III Para A Part A, Clause 6 (ii).

under Regulation 30(4).[58] SEBI recently clarified the scope of pending litigation or disputes through its Circular.[59] It states that a listed entity must notify the stock exchange(s) if it or its management is involved in "*any litigation, assessment, adjudication, arbitration, or dispute in conciliation proceedings, or if it is the subject of any of these actions, including any interim or ad-interim orders passed in favor (sic.) of or against the listed entity*", and the outcome of these may reasonably have an impact.

In insolvency cases, when an operational creditor submits an insolvency application, an AA must adjudicate whether the application can be admitted. Thus, this constitutes a pending dispute or litigation. However, to determine if such a filing warrants disclosure, it should meet the following materiality criteria under Regulation 30(4) of the LODR Regulations:

1. Whether the failure to disclose an event/information may cause the discontinuance or adjustment of publicly available information; or

2. Whether the failure to disclose an event/information may result in a major market reaction if the omission is found later; or

[58] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 Schedule III Para B of Part A, Clause 8.

[59] SEBI, Disclosure of material events / information by listed entities under Regulations 30 and 30A of Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015' Circular No. SEBI/HO/CFD/CFD-PoD-1/P/CIR/2023/123 dated 13-7-2023; See also, *Rourkela Steel Syndicate vs Metistech Fabricators Pvt. Ltd.* Company Appeal (AT)(Insolvency) No. 924 of 2022.

3. Whether the failure to disclose an event/information would meet the quantitative thresholds, or

4. An event or information may be deemed material by the board of directors even if it does not meet any of the standards mentioned above.

The term "*material*" or "*materiality*" encompasses any factor that has the potential to influence an investor's decision regarding an investment, and its determination is contingent upon the specifics of each situation.[60] In the securities market, predicting whether an event is or will be material is highly complex and challenging.[61] Thus, SEBI amended the LODR Regulations and introduced quantitative thresholds in Regulation 30(4) to determine the materiality of an event/information.[62] This amendment significantly modified the disclosure framework by requiring disclosure of an event or information if the value or the expected impact in terms of value exceeds certain percentages of the listed entity's turnover, net worth, and the average of the absolute value of profit or loss after tax. It eliminates divergent interpretations and reduces ambiguity for disclosure of events under Para B.[63]

---

[60] Suzlon Energy Ltd. v. SEBI, Appeal No. 201 of 2018, Order dated 3 May 2021.
[61] Eric Bonabeau, *Predicting the Unpredictable,* 80(3) HARV. BUS. REV. 109 (2002).
[62] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Regulation 30(4)(i)(c).
[63] SEBI, Memorandum on Amendments to requirements for disclosure of material events or information by listed entities under LODR Regulations, 2015

A listed entity may not deem the filing of an operational creditor's insolvency application to be a material event if it does not meet the quantitative thresholds.[64] However, the duty to disclose information relating to the financial health of a company is an integral issue and generally has received much attention.[65] Lawsuits and related claims which affect the integrity of a company must be disclosed based on three reasons below:

First, though these insolvency filings may not immediately impact a company's net worth, turnover, or profits, they initiate market scepticism, and investor sentiment for public entities is sensitive.[66] Insolvency filings typically lead to a reduction in a company's valuation.[67] For instance, when Café Coffee Day disclosed that an insolvency application was filed against it, it resulted in a significant crash in its share price, which was more than 17%.[68]

---

https://www.sebi.gov.in/sebi_data/meetingfiles/apr-2023/1681703089597_1.pdf at 5 ("**SEBI Memorandum**").

[64] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Regulation 30(4)(i)(c).

[65] Ferrara, Starr & Steinberg, *Disclosure of Information Bearing on Management Integrity and Competence*. 76 NW. U. L. REV. 555 (1981).

[66] Gideon Ewers, *Lilium Shares Crash as Insolvency of Subsidiaries Announced*, ROTOR HUB INTERNATIONAL, 25 October 2024, https://www.rotorhub.com/lilium-shares-crash-as-insolvency-of-subsidiaries-announced/.

[67] Banikinkar Pattanayak, '*IBC Recovery on Companies' Fair Values Up, Claims Down*' *THE ECONOMIC TIMES,* 16 NOVEMBER 2024, https://economictimes.indiatimes.com/industry/banking/finance/ibc-recovery-on-companies-fair-values-up-claims-down/articleshow/115343826.cms?from=mdr .

[68] Asit Manohar, *Coffee Day Shares Crash 17% after IDBI Trusteeship's Lawsuit at NCLT for Alleged ₹228 Crore Default*, (MINT, 11 September 2023), https://www.livemint.com/market/stock-market-news/coffee-day-shares-crash-17-after-idbi-trusteeships-lawsuit-at-nclt-for-alleged-rs-228-crore-default-11694406487258.html.

In a study on the impact of lawsuits on a listed entity, Bhagat et al. found that, on average, listed companies lose nearly 1% of their value on the day a lawsuit is filed against them, with losses rising in value to 1.73% for suits brought by government agencies.[69] Filing insolvency applications negatively impacts credit ratings and increases credit risk, prompting lenders to adopt stricter borrowing conditions and higher interest rates,[70] which may gradually erode the company's net worth.[71] While turnover might not be immediately impacted, reputational damage that's caused can deter customers and suppliers,[72] constraining revenue and operational continuity.

Second, an AA must decide on an insolvency application within fourteen days of its receipt.[73] However, this timeline is "*procedural and directory*"[74] and most delays occur in the admission stage of CIRP applications.[75] This delay in admitting an operational creditor's application

---

[69] Sanjai Bhagat et. al, *The Shareholder Wealth Implications of Corporate Lawsuits*, 27 FIN. MGMT. 25 (1998).
[70] Q Yuan and Y Zhang, *Do Banks Price Litigation Risk in Debt Contracting? Evidence from Class Action Lawsuits*, 42(9-10) J. BUS. FIN. ACC. 1310 (2015).
[71] Matteo Arena and Stephen Ferris, *A Survey of Litigation in Corporate Finance*, 43(1) *MANAGERIAL FIN.* 4 (2017).
[72] J M Karpoff and J R Lott, *The Reputational Penalty Firms Bear from Committing Criminal Fraud,* (36(2) J. LAW. ECON. 757 1993).
[73] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 9(5) (India).
[74] Surendra Trading Company v. Juggilal Kamlapat Jute Mills Co. Ltd. & Ors, NCLAT Delhi Company Appeal (AT) (Insolvency) No. 189 of 2018 (43).
[75] Ministry of Corporate Affairs Standing Committee on Finance, *Implementation of Insolvency and Bankruptcy Code- Pitfalls and Solutions* (Thirty-Second Report 2020-2021) (hereinafter "**MCA Report on IBC**"); Insolvency and Bankruptcy Board of India, *Consultation paper on issues related to reducing delays in the corporate insolvency resolution process* (April 13, 2022) https://ibbi.gov.in/uploads/whatsnew/72a560ce5697bbaeef62ce5893a3f1ad.pdf.

leads to an information asymmetry in the market, leaving investors in the dark till the AA decides on a s.9 application. The significant delays in adjudication by the AA, combined with the continued control of the listed entity by defaulting promoters, create opportunities for value shifting, diversion of funds, and transfer of assets.[76] These actions can amplify the impact of the insolvency process beyond the initially expected impact value, posing greater risks.

Third, Clause 16(c) under Para A of Part A of Schedule III mandates disclosure of "*Admission of application by the Tribunal, ... or rejection or withdrawal, as applicable*".[77] However, it is not clear whether the rejection or withdrawal clauses refer to an application filed by any creditor or only those filed by a corporate applicant and financial creditors. Requiring the disclosure of an operational creditor's application withdrawal or rejection seems illogical when there was no initial requirement to disclose its filing. The ambiguity in the clause for the lack of specificity could be taken to imply the disclosure of any insolvency application.

Apart from the above reasons derived from a joint reading of Schedule III and Regulation 30(4) of the LODR Regulations, the filing of S. 9 IBC applications may also require disclosure under Regulation 30(12). This provision acts as a catch-all clause and ensures that no material event escapes disclosure simply because it is not explicitly specified. It serves as a

---

[76] *Id.*

[77] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 Schedule III Para A of Part A, Clause 16(c).

safeguard to ensure that listed companies provide all material information.[78] Regulation 30(12) states that if an event occurs or information in possession of the listed entity that is not explicitly mentioned in Paras A or B of Part A of Schedule III but would have a material effect in the market, the listed entity must make timely and adequate disclosures regarding the event or such information. The Boards of these companies are authorised to make these disclosures if they deem it fit.[79]

An outcome of an insolvency proceeding may be substantial changes to a corporate entity's ownership, management, and overall course of business. These events have the potential to significantly impact share prices, market dynamics, and investment choices. Regulation 30(12) fills in any possible gaps in the lists of occurrences that fall into predetermined categories and need to be disclosed. It empowers companies to proactively disclose information critical for informed decision-making by investors. Hence, disclosures regarding the filing of a S.9 application can also be covered here.

---

[78] SEBI Consultation Paper, Review of disclosure requirements for material events or information under SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, https://www.sebi.gov.in/web/?file=https://www.sebi.gov.in/sebi_data/attachdocs/nov-2022/1668240795810.pdf#page=1&zoom=page-width,-10,749, (last visited Apr. 18, 2024).

[79] SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, Regulation 30(4)(i)(d).

As a result, pending litigations often have the potential to adversely affect a company's reputation or share price.[80] The inherent difficulty in assessing the potential impact of pending litigation, combined with the lengthy delays in adjudication, highlights the risks of relying on discretion in these matters. While objective criteria might seem like a reliable approach, it is complicated to predict the future impact of an insolvency application when adjudication occurs long after the filing. In other words, what may not be a material event today may later appear as a missed obligation, suggesting that discretion in such cases is not advisable.

Additionally, though an event/information may not be quantitatively material because it does not significantly impact an issuer's assets, it is often qualitatively material in that it reflects on the quality of corporate management.[81] SEBI provides that it is a best practice to disclose events or information with the best estimate at hand rather than allowing rumours/speculation, especially where assessment of materiality may take time.[82]

If an event is required to be disclosed later (By virtue of then meeting the quantitative thresholds under the materiality guidelines under Regulation 30(4)(c) of the LODR Regulations.), it could trigger a number of other violations, like violating the SEBI PIT Regulations and the SEBI Act. For instance, the lack of disclosure requirements creates an

---

[80] Robert G. Eccles, Scott C. Newquist, and Roland Schatz, *Reputation and Its Risks* (85(2) HARV. BUS. REV. 104 (2007), https://hbr.org/2007/02/reputation-and-its-risks ; *Supra* note 57, *Shilpi Cable* (29.2).
[81] *Supra* note 66.
[82] *Supra* note 64 at 9.

opportunity for insider trading.[83] Thus, it is prudent to exercise caution and take a conservative approach while determining whether to disclose, according to the tenet that "disclose rather than avoid/hide."[84] Taking into account the repercussions of non-compliance in the securities market, this strategy is consistent with the goal and purpose of Regulation 30.

II. SECTION 9 APPLICATION AS A 'MATERIAL EVENT': AN ANALYSIS OF PRECEDENTS

This chapter explores judicial precedents requiring listed companies to disclose the filing of operational creditors' insolvency applications. It examines two cases decided by SEBI, which are empirically exhaustive on this topic, and they impose a de facto requirement for making disclosures on this issue mandatory. It then focuses on a practical example of a company's voluntary disclosure.

A. THE PRECEDENTS

The first precedent to examine is the adjudication order in the matter of insider trading activities is the case of *Shilpi Cable Technologies Ltd.* ("**Shilpi Cables**")[85] In this case, the operational creditor issued a demand

---

[83] SEBI (Prohibition of Insider Trading) Regulations, 2015, Regulation 3(1).

[84] K.R. Chandrate, Impact on Listed Companies of Amendments to Regulation 30 of Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015' (*ICSI* 2023) <https://www.icsi.edu/media/webmodules/CSJ/August/16.pdf> accessed 06 May 2024; *See* Laura & Lowry, Michelle & Shu, Susan, *Does disclosure deter or trigger litigation?* 39 J. ACCT. & ECON. 506–07 (2005).

[85] Shilpi Cable (n 57).

notice and subsequently filed an application under S.9 of the IBC to initiate CIRP against Shilpi Cable Technologies Ltd. ("**SCTL**"). Despite these developments, SCTL only disclosed the creditor's insolvency petition after a considerable delay.[86] In deciding on disclosure requirements under LODR, the Adjudication Officer ("**AO**") relied on Regulation 30 of the LODR Regulations read with the then Clause 11 of Para A of Part A of Schedule III. Clause 11 required disclosure of events having "*Reference to BIFR and winding-up petition filed by any party/creditors*".[87] Clause 11 was amended and the words "*reference to BIFR and*" was omitted by the SEBI LODR (Second Amendment) Regulations, 2023 w.e.f. 15 July 2023.[88] In Shilpi Cables, the AO is likely to have read 'BIFR and winding up petitions' to include events under CIRP. This reading is tenable as the IBC was introduced in 2016 as a successor to Sick Industrial Companies (Special Provisions) Act, 1985, which governed Board for Industrial and Financial Reconstruction, and both legislations have a fundamentally common aim of reviving and rehabilitating companies in financial distress.[89]

The AO held that SCTL failed to disclose not only the operational creditor's insolvency application but also went a step ahead to hold nondisclosure of the receipt of the initial demand notice under S.8.[90] The AO concluded that the receipt of a demand notice, though not equivalent

---

[86] Shilpi Cable (n 57) (87, 91-94).
[87] SEBI LODR (Second Amendment) Regulations, 2023 w.e.f. 15 July 2023. See, *Shilpi Cable* (n 57) (85-86).
[88] SEBI LODR (Second Amendment) Regulations, 2023
[89] Swiss Ribbons (n 31) (75); Preamble of Sick Industrial Companies (Special Provisions) Act 1985 and Preamble of Insolvency and Bankruptcy Code 2016.
[90] *Supra* note 57 (87).

to the initiation of CIRP, signals a default by the company and a possible CIRP in the near future.[91] Listed companies, therefore, have an obligation to promptly disclose both the receipt of the demand notice and the filing of an insolvency application against them.[92]

Thus, this case is significant as it highlights SEBI's stance that a listed company must mandatorily disclose these two events: *first*, the receipt of a demand notice and *second*, the filing of an insolvency application. As a result, this case casts an obligation to disclose these events in practice, even when the Regulations are silent on this.

Building on the principles established in *Shilpi Cables*, another significant case came up for adjudication in September 2024 before SEBI. In *BGR Energy Systems Limited* ("**BGR Energy**"),[93] issues concerned multiple violations of disclosure requirements under LODR Regulations. One of the issues was regarding the company's failure to disclose an operational creditor's S. 9 IBC application for initiating CIRP.

The AO held that BGR Ltd had violated disclosure requirements per LODR Regulation 30, read with Clause 16(b) of Para A, Part A of Schedule III and imposed a penalty of INR 9,00,000.[94] The AO reasoned that failing to inform the stock exchanges of an insolvency application being

---

[91] *Id.* (29.9).
[92] *Id.* (30.2).
[93] *In the matter of BGR Energy Systems Limited* SEBI Adjudication Order Ref No: Order/BM/RK/2024-25/30809.
[94] *Id.* (33-37 and 84).

filed against a public company constitutes a violation of LODR Regulations and ordered this disclosure as a mandatory one. Clause 16 of Para A provides for the disclosure of CIRP-related events of a listed company. Interestingly, Clause 16(b) requires mandatory disclosure of a financial creditor's application for initiating CIRP.[95]

Therefore, BGR Energy reiterates SEBI's expectation for a mandatory disclosure of operational creditors' insolvency filings, despite not having any such requirement in the regulations. This case signifies a regulatory shift, treating operational and financial creditors' insolvency applications on the same footing, at least in practice. It imposes this practical disclosure requirement for insolvency-related disclosures, regardless of the creditor type.

Having examined the above precedents, we now turn to an example that further illustrates the practical implementation of disclosure norms even before these cases.

Praxis Home Reality Limited ("**PHRL**")[96] provides an interesting case study regarding the practice of disclosure norms. While LODR regulations do not explicitly require disclosure of applications filed by operational creditors, PHRL chose to disclose the application filed by an operational creditor under the heading "*Application by Financial Creditors*", i.e., under

[95] Clause 16(b) of Para A of Part A of Schedule III of LODR Regulations.

[96] Praxis Home Retail Limited, '*Disclosure in terms of Regulation 30 of SEBI (Listing Obligation and Disclosure Requirements) Regulations 2015, as amended ("Listing Regulations")*' 18 April 2021 (SEBI BSE-NSE/Reg-30/FY2021-22/02), https://www.bseindia.com/xml-data/corpfiling/AttachHis/27810836-93f3-4b1c-9f20-f8fe7bcf95f9.pdf.

Clause 16(b) of Para A of Part A of Schedule III.[97] This example highlights a key point: even without a specific mandate, some companies recognised the importance of such transparency and have actively been disclosing CIRP-related events to stock exchanges.

These cases highlight the inconsistency between the LODR Regulations, which distinguish between operational and financial creditors, and SEBI's practical treatment of their disclosures as equivalent. This gap between legal provisions and actual practice creates confusion, inconsistencies in compliance, and uneven disclosures across companies, leading to penalties at times. This strongly calls for the need to re-evaluate the regulatory framework to align disclosure requirements for operational creditors with the current trends.

III. CONCLUSION

This paper examined the regulatory lacuna in the SEBI (LODR) Regulations concerning the non-mandatory disclosure of insolvency applications filed by operational creditors under s.9 of the IBC. We argued that the filing of such applications should be mandatorily disclosed as a material event to protect investors and ensure market integrity.

Despite the absence of a specific statutory requirement, Regulation 30, when read alongside Paras A and B of Schedule III of LODR Regulations, creates a de facto obligation. Paras A and B of Schedule III of

[97] *Id.* at 2.

LODR Regulations require a listed company to disclose any defaults and pending litigation, respectively. These requirements mandate disclosure of a CIRP application being filed by an operational creditor.

A company may strategically hold off disclosing certain events to preserve its competitiveness, but we argued for its disclosure considering two key objectives: protecting the company from potential penalties and upholding the principle of investor protection. Such regulatory clarity becomes essential where disclosures are necessitated by either direct or indirect requirements under the LODR Regulations, particularly in light of SEBI's interpretive stance in its adjudication orders. Lastly, it should be noted that the distinction between financial and operational creditors in disclosure requirements is incongruous. The consequence of a CIRP initiated by any creditor poses an equivalent threat to the existence of the corporate debtor. The current asymmetry in disclosure obligations between financial and operational creditors is unjustified, especially after the upward revision of the default threshold to □1 crore. Given the high stakes involved and the systemic risk posed by non-disclosure, regulatory clarity is overdue.

Thus, it is recommended that SEBI may consider incorporating an operational creditor's application in Para A of Schedule III. This inclusion would promote transparency and eliminate confusion and information asymmetry in the market, thus preventing certain entities from gaining unfair advantages due to a lack of disclosure requirements. It also aligns with the spirit of SEBI's initial proposal, which provided for disclosures of

these applications. Thus, LODR Regulations must be suitably tailored to promote insolvency resolutions and protect the interests of investors in securities issued by such corporate debtors.

NLUJ Law Review
Charchit Pathak, *Regulatory Responses to Deepfakes in the Electoral Process: A Constitutional and Statutory Evaluation under Indian Law,* 12(1) NLUJ L. Rev. 38 (2026)

REGULATORY RESPONSES TO DEEPFAKES IN THE ELECTORAL PROCESS: A CONSTITUTIONAL AND STATUTORY EVALUATION UNDER INDIAN LAW

~ Charchit Pathak[*]

ABSTRACT

The emergence of deepfakes and artificial-intelligence-developed synthetic media is a serious threat to democratic elections. Deepfakes imitate biometric characteristics like voice and facial expressions, which is unlike conventional misinformation. Deepfakes can hardly be distinguished because they appear almost real. This aspect has been shown by their inclusion in the general elections in India 2024, which highlighted the need for better laws to cover this new threat, as the current provisions in effect in the Bhartiya Nyaya Sanhita, the Information Technology Act, and the Representation of the People Act are insufficient to combat this issue. This paper critically argues the regulatory gap pertaining to electoral deepfakes in India, contrasting the responses elsewhere through EU regulations of the AI Act, state laws of the USA, and deep synthesis laws in China, and analysing constitutional conflicts of free speech and electoral integrity. It proposes statutory reforms to specifically target AI-manipulated electoral content, additional institutional capabilities to the Election Commission, and platform responsibilities for watermarked and synthetic media that respondents predict. The combination of legal,

[*] Charchit Pathak is a fourth-year B.A LL.B. (Hons.), student at Symbiosis Law School, Hyderabad.

technological, and institutional changes enables India to protect democratic procedures against the disruptive capabilities of deepfakes.

TABLE OF CONTENTS

I. INTRODUCTION 42
II. DEEPFAKES & THE ELECTORAL CONTEXT 46
A. WHAT ARE DEEPFAKES, AND WHAT ARE THE RISKS OF DEEPFAKES IN ELECTIONS? 46
B. INDIA'S 2024 ELECTIONS: A CASE STUDY 47
III. INDIAN LEGAL SYSTEM 51
A. CRIMINAL & CYBER LAW: BNS AND IT ACT 51
B. ELECTORAL LAW: REPRESENTATION OF THE PEOPLE ACT AND ELECTION COMMISSION 53
C. JUDICIAL APPROACH AND EVIDENTIARY ISSUES 54
IV. CONSTITUTIONAL DIMENSIONS 56
A. THE INDEPENDENCE OF ELECTION AND THE FREEDOM OF SPEECH 56
B. ARTICLE 21 RIGHT TO REPUTATION AND PRIVACY 57
C. THE INFORMED CHOICE AND THE RIGHT TO KNOW OF THE VOTER 59
V. COMPARATIVE INTERNATIONAL APPROACHES 60
A. WORLDWIDE ELECTORAL DEEPFAKE SPREAD 61
B. EUROPEAN UNION: TRANSPARENCY AND PLATFORM RESPONSIBILITY 63
C. UNITED STATES: CRIMINALISATION AT THE STATE LEVEL 64
D. CHINA: MANDATORY WATERMARKING AND REAL-NAME VERIFICATION 65

E. AUSTRALIA: INTEGRITY AND DISINFORMATION CODES OF ELECTORAL CONDUCT 66

F. LESSONS FOR INDIA 67

VI. IDENTIFICATION OF GAPS AND RECOMMENDATIONS ..69

A. LACUNAS IN THE PRESENT LEGAL SYSTEM 69

B. REFORM SUGGESTIONS 70

C. BALANCED INDIAN MODEL 72

VII. CONCLUSION 73

I. INTRODUCTION

Technology has always been a sword with two edges in electoral politics. On the one hand, it has allowed democratic participation, on the other hand, it has provided an open door to manipulation. Since the distribution of pamphlets at the colonial elections to the televised campaigns of the 1980s,[1] and the social media-based elections of the past decade, every new technology has changed the dynamics between political candidates and the elections. With the appearance of artificial intelligence, however, the point of inflexion is achieved. This shift is most clearly visible in the emergence of deepfakes which are hyper-realistic audio-visual fictions created with deep learning algorithms. They are not only an extension of misinformation but an essential destabilizing of democratic discourse.

Deepfakes use biometric authenticity, unlike traditional fake news, which can give away its untruthfulness by being inconsistent in the text or having zero credibility. A doctored video of a political leader addressing in a local dialect or an Artificial Intelligence ("**AI**") generated voice that distorts campaign promises will have a much stronger persuasive influence than computerized forms of text and photoshopped photos. This voice, gestures, and emotion imitation make deepfakes the most dangerous during

[1] Amogh Dhar Sharma, *Concertina Wires and the Crocodile: The General Elections of 1984 and the Rise of Political Marketing in India*, THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE (Mar. 13, 2023), https://blogs.lse.ac.uk/southasia/2023/03/13/concertina-wires-and-the-crocodile-the-general-elections-of-1984-and-the-rise-of-political-marketing-in-india/.

election time, when voters must trust and believe in the authenticity of the message.

The example of the 2024 general elections in India evidences how urgent this concern is. There were reports of AI-created campaign videos made to suit the electorate in particular regions, and political leaders apparently speaking dialects they had never before used. Some of them were harmless, so-called AI-translations created with consent, whereas others were spread without agreement, blurring the line between acceptable innovation and malicious manipulation.[2] The Election Commission of India ("**ECI**") sent advisories to parties that they should not use deepfakes, but this was not enough, since it cannot be enforced.[3] What is more disturbing is that the voters were not equipped with the means of discerning genuine political messages and fake counterfeits, and there are concerns about the informed electoral choice.

Currently, India uses outdated and fragmented legislation to deal with this challenge. Defamation, forgery, and impersonation fall under the category of offences covered by the Bharatiya Nyaya Sanhita, 2023 ("**BNS**") though these are inapplicable to deepfakes since it is hard to prove

---

[2] Anandi Choudhhari, *Depp Fakes, Deeper Impacts: AI Role in the 2024 Indian General Election and Beyond*, GLOBAL NETWORK ON EXTREMISM & TECHNOLOGY (Sept. 11, 2024), https://gnet-research.org/2024/09/11/deep-fakes-deeper-impacts-ais-role-in-the-2024-indian-general-election-and-beyond/.

[3] Aditi Agrawal, *Remove deepfakes within 3 hours of being notified: Election Commission to political parties*, HINDUSTAN TIMES (May 7, 2024), https://www.hindustantimes.com/india-news/remove-deepfakes-within-3-hours-of-being-notified-election-commission-to-political-parties-101715023235465.html.

culpability and intent. Online content is regulated through the Information Technology Act, 2000 ("**IT Act**") and the Information Technology Rules, 2021 ("**IT Rules**"), which are aimed at obscenity, national security, and intermediary liability, but not electoral misinformation. Representation of the People Act, 1951 ("**RPA**"), contains a ban on false statements and corrupt practices, but it is still anchored in the pre-digital past and fails to presuppose the manipulation with the help of AI. Although the ECI is charged with conducting free and fair elections under the constitution, it does not have proper statutory mechanisms to counter synthetic media.

This is in comparison to other jurisdictions that have started innovating. The Artificial Intelligence Act, 2024 ("**AI Act**"), developed by the European Union,[4] classifies deepfakes as high-risk AI and requires transparency and labelling. A number of states in the United States have criminalized deepfakes related to elections during campaigns, since they can influence the opinion of the voters.[5] China has taken this further by requiring the labelling of all AI-generated content and conspicuous watermarks.[6] India is, however, lagging behind as no special laws are focused on electoral deepfakes.

The consequences of such a gap are not only technological, but also constitutional. Deepfakes attack the fundamental democratic freedoms: the

---

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council, 13 June 2024 on Artificial Intelligence (Artificial Intelligence Act) , 2024 O.J. (L 168) 1 (EU).
[5] Chris Habels Gray, *Political Deepfakes and Elections*, Free Speech Center (Jan 11, 2025), https://firstamendment.mtsu.edu/article/political-deepfakes-and-elections/.
[6] Yan Luo & Xuezi Dan, *China Releases New Labeling Requirements for Ai-Generated Content*, CONVIGHTON(Mar.18,2025),https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/.

right to free speech, the right to reputation, the right to privacy, and above all, the right of people to vote, and make an informed choice. The conflict between the role of regulating fake media and the principles of free speech guaranteed under Article 19(1)(a) of the Constitution,[7] is a very difficult and challenging legal issue. The Supreme Court jurisprudence of *Romesh Thappar*[8] to *Puttaswamy*[9] demonstrates the sacrosanctity of freedom of expression as well as the importance of democratic integrity.

This paper proposes that reliance on general provisions of criminal law and content regulation is not sufficient. This must be done in a wholesome manner by tying together changes in the statutory codes to the Representation of the People Act, strengthening the Election Commission, and active responsibilities by digital platforms. An electoral integrity hybrid model that incorporates legal reform, technology-based solutions, and voter literacy is the only method of preserving electoral integrity under the conditions of synthetic media. The paper is structured in the following way. Part II looks at what deepfakes are in the electoral context and how they can be differentiated from other misinformation. Part III examines the legal system of India today and its failures. Part IV places India in the global regulatory trends. Part V has a look at constitutional aspects and the balancing of fundamental rights. Part VI enumerates some of the main regulatory gaps and suggests specific reform proposals. The paper ends

---

[7] INDIA CONST. art. 19, cl. 1(a).
[8] Romesh Thappar v. The State of Madras, 1950 SCC 436.
[9] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., 2017 10 SCC 1.

with a note on the urgency needed to reform before the next general election cycle in India.

II. DEEPFAKES & THE ELECTORAL CONTEXT

A. WHAT ARE DEEPFAKES, AND WHAT ARE THE RISKS OF DEEPFAKES IN ELECTIONS?

Deepfakes have been among the most disruptive artificial intelligence uses in recent years. These hyper-realistic synthetic media are generated mostly via Generative Adversarial Networks ("**GANs**") and imitate the human voice, expressions, and gestures to a tremendous degree.[10] In that sense, they are quite different in principle from previous versions of digital manipulation, such as photoshopping or rudimentary video editing. A deepfake video of a political leader giving a fake speech can leave a voter with little or no chance to differentiate real and fake.

That is why researchers view deepfakes as a direct threat to democracy, largely due to a concept of 'Liar's Dividend' elucidated by Bobby Chesney and Danielle Citron. It is a phenomenon that occurs when public awareness of deepfakes causes skepticism, which impacts individuals to discredit authentic recordings as fabricated.[11] Its risk is twofold: on the one hand, deepfakes that have been maliciously created can be used to mislead voters into believing false information; on the other hand, political

---

[10] GAO-20-379SP, *Science & Tech Spotlight: Deepfakes*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, (Feb. 20, 2020), https://www.gao.gov/products/gao-20-379sp.

[11] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* 109 CALIFORNIA L. REV. 1753 (2019).

actors can also use the availability of deepfake technology to avoid responsibility when they make authentic but humiliating claims.

This phenomenon displays a major threat to the constitutional right of voters to make informed decisions, which is an essential part of Article 19(1)(a) of the Constitution, which talks about the freedom of speech and expression. This misconstruction of the "marketplace of ideas" through deepfakes undermines the integrity of free and fair elections and thereby violates the Constitution's basic structure. As synthetic media manipulates voters, they impair voters' ability to act independently, thereby eroding the very foundation of electoral democracy.

B. INDIA'S 2024 ELECTIONS: A CASE STUDY

The 2024 Lok Sabha elections in India were the first massive experience with electoral deepfakes. The political campaigns actively utilized AI-based content to reach a greater number of voters.[12] A prominent example of this usage was the BJP leader Manoj Tiwari delivering a speech translated by AI into Haryanvi, a language which he does not speak fluently.[13] This sanctioned application is freely revealed by

---

[12] Vandinika Shukla & Bruce Schneier, *India's Latest Election Embraced AI Technology. Here Are Some Ways It Was Used Constructively*, PBS NEWS (Jun. 12, 2024), https://www.pbs.org/newshour/world/indias-latest-election-embraced-ai-technology-here-are-some-ways-it-was-used-constructively; Deeplina Banerjee et. al., *In Indian Election, AI Amplifies Political Reach but Magnifies Disinformation*, ASIA PACIFIC FOUNDATION OF CANADA (Jun. 5, 2024), https://www.asiapacific.ca/publication/indian-election-use-of-ai-political-campaigns-voter-engagement.

[13] Mariyam Alavi, *BJP Shared Deepfake Video On WhatsApp During Delhi Campaign*, NDTV NEWS (Feb. 20, 2020), https://www.ndtv.com/india-news/in-bjps-deepfake-video-shared-on-whatsapp-manoj-tiwari-speaks-in-2-languages-2182923.

campaign managers, showing how AI can democratize access through overcoming linguistic obstacles. But the dark side came out shortly. Several unauthorized deepfakes were widely spread on social media in which leaders were shown to be saying something that they had never said. Let's suppose a video clip of a senior opposition party leader using abusive language against a community, which was rapidly circulated on WhatsApp groups, Instagram, Twitter (now X), how worse it can impact the democratic electoral process and mislead the community at large or can also potentially cause communal violences.

Similarly, several high profile instances involved a doctored video of the Union Home Minister Amit Shah, which misrepresented him as advocating the removal of reservation systems for Scheduled Castes and Tribes, publication of such a video led to a police investigation and served as a reminder as to the potential for synthetic media in provoking social unrest.[14] Moreover, actors from Bollywood, including Ranveer Singh and Aamir Khan, were also misrepresented in AI-generated videos, which contained false representations of them endorsing the Indian National Congress and expressing discontent with the Prime Minister. These incidents served as concrete examples of the ease with which celebrity

[14] TOI News Desk, *Amit Shah Fake Video Case: Twitter Withholds Jharkhand Congress Handle*, TIMES OF INDIA (May 1, 2024), https://timesofindia.indiatimes.com/india/amit-shah-fake-video-case-twitter-withholds-jharkhand-congress-handle/articleshow/109759634.cms; NEWS9 Live, *The Deepfake Dilemma: Amit Shah and the Fake Video Controversy Explained*, NEWS9 (Apr. 30, 2024), https://www.youtube.com/watch?v=2x8hBfXlO64.

endorsements can be manipulated by political parties to confuse voters through misleading and fabricated endorsement campaigns.[15]

Fact-checking organisations such as AltNews and BoomLive exposed these videos as fake, but their correction reached only to a fraction of the original audience influenced or have seen the fake content, and by the time the truth was available it was too late to undo the damage already done by such content.[16] The ECI took note of how grave the problem had become, and on 6 May 2024, 16 January 2025, and 24 October 2025, released some advisory circulars to political parties urging them to be careful when using AI-generated media and not to produce misleading content.[17] However, the directive was primarily restrictive due to its

---

[15] Amir Khan & Ranveer Singh Criticising PM Modi! Think Again, That's Deepfake Drama, ECONOMIC TIMES (Apr. 22, 2024), https://economictimes.indiatimes.com/news/elections/lok-sabha/india/deepfakes-of-bollywood-stars-spark-worries-of-ai-meddling-in-india-election/articleshow/109487075.cms; Varun Borugadda, *Edited Videos of Amir Khan Circulated as Him Promoting Congress Manifesto and Cautioning Against 'Jumlas'*, FACTLY (Apr. 17, 2024), https://factly.in/edited-video-of-aamir-khans-satyameva-jayate-promo-falsely-presented-as-a-warning-against-jumlas/.

[16] Srijit Das, *Video of Ranveer Singh Criticising PM Modi Is a Deepfake AI Voice Clone*, BOOM (Apr. 18, 2024), https://www.boomlive.in/fact-check/viral-video-bollywood-actor-ranveer-singh-congress-campaign-lok-sabha-elections-claim-social-media-24940; Ritesh Gautam, *Emerging AI Techniques and Dissemination of Misinformation: A Qualitative Approach*, 2 INT'L J. GLOB. RSCH. INNOVS. & TECH. 52-60 (2024), https://www.inspirajournals.com/uploads/Issues/1993708502.pdf; Adnan Bhat, *'Chapfakes,' not Deepfakes, Spread Election Lies in India*, Context (Jun. 3, 2024), https://www.inspirajournals.com/uploads/Issues/1993708502.pdf.

[17] Anuj Chandak, *Responsible and ethical use of social media platforms and strict avoidance of any wrongful use by political parties and their representatives during MCC period in General Elections and by-elections,* ELECTION COMMISSION OF INDIA (May. 6, 2024), https://elections24.eci.gov.in/docs/2eJLyv9x2w.pdf; S.B.Joshi, *Advisory for labelling synthetic/AI generated content used by Political Parties for election campaigning,* ELECTION COMMISSION OF INDIA, (Jan.16, 2025),

operation under the Model Code of Conduct ("**MCC**"), because it does not have statutory authority and therefore relies on moral persuasion, not legal consequences. As such, the Commission could only issue warnings or censures rather than issuing criminal sanctions. Additionally, neither the Representation of the People Act of 1951 nor any other law specifically categorizes or includes deepfakes and synthetic media under any category, leaving no clear options for law enforcement agencies to use existing provisions on false statements and related offences. Furthermore, due to a lack of independent infrastructure to monitor deepfakes in real-time, the Commission is limited to using reactive strategies in combating them, which often failed to remain ahead of the tidal wave of misinformation that was being disseminated.

In conclusion, the 2024 elections thus revealed three weak links of India's electoral democracy. Firstly, there is no definition of synthetic media and deepfakes in the Indian legislature. Secondly, the ECI does not have sufficient technical ability to detect deepfakes in real time. Lastly, Indian voters are particularly susceptible to deception due to low levels of media literacy.

---

https://www.eci.gov.in/ecibackend/public/api/download?url=LMAhAK6sOPBp%2FNFF0iRfXbEB1EVSLT41NNLRjYNJJP1KivrUxbfqkDatmHy12e%2FzGjJMI0%2FjETs7fjrM8lYn4ipTqYtDEvVosG8Bae5QB8%2Fj5TBF9Esc2hlzORgYtkmzyKzGsKzKlbBW8rJeM%2FfYFA%3D%3D; Anuj Chandak, *Advisory on responsible use and disclosure of synthetically generated information and AI-generated content during elections,* (Oct. 24, 2025), ELECTION COMMISSION OF INDIA, https://ceogoa.nic.in/pdf/Advisory_%20AI.pdf.

III. INDIAN LEGAL SYSTEM

A. CRIMINAL & CYBER LAW: BNS AND IT ACT

The Bharatiya Nyaya Sanhita ("**BNS**") and the IT Act are the first line of defence that India has against malicious deepfakes. Some of the crimes that have been criminalized by the provisions of the BNS include forgery under Sections 336-338,[18] defamation under Sections 356,[19] and impersonation under Sections 319.[20] Although, in principle they can be applied to deepfake materials, these regulations were formulated during the pre-digital age and do not consider the use of AI to create a manipulative effect. The main challenge here is the issue of attribution: a deepfake can be done anonymously, shared over encrypted systems, and stored on overseas servers, which makes identifying the culprit almost impossible.

On the same note, the IT Act has crimes, including identity theft under Section 66C,[21] publication of obscene material under Section 67,[22] and intermediary liability under Section 79.[23] The IT Rules, 2021,[24] also require due diligence by the social media platforms in taking down unlawful content at the direction of the government. Nevertheless, they are mostly

---

[18] The Bharatiya Nyaya Sanhita, 2023, §336-338.
[19] *Id* §356.
[20] *Id* §319.
[21] The Information Technology Act, 2000, §66C.
[22] *Id* §67.
[23] *Id* §79.
[24] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

focused on morality, pornography, and national security, but not on the manipulation of elections.

As these provisions are dependent upon a formal complaint, which requires that an order of removal be issued, the relief provided through this framework remains inherently reactive. This inherent process leads to the removal of the content only after considerable harm has occurred. Retrospective remedies will not suffice within the fast-paced electoral process, as the rapid dissemination of deepfakes is frequently faster than the ability of laws to intervene. Therefore, once the content is removed, the false narrative has already affected the voters, meaning that any corrective measures taken are of little value.

The Apex Court in *Shreya Singhal v. Union of India,*[25] established significant constitutional protections against regulation of free speech via electronic means, it was found that Section 66A of the IT Act was unconstitutionally vague. The justices determined that vague terms like "grossly offensive" enabled arbitrary enforcement and fostered a "chilling effect" on legitimate speech through the threat of prosecution. Additionally, the ruling clarified the degree of liability of online intermediaries under Section 79 by holding that the intermediary must only take down content when there is "actual knowledge", as evidenced by either a court order or a direction from a government agency, user complaints do not equate to actual knowledge. This standard creates a significant challenge for the regulation of deepfake electoral content at present. On one hand,

[25] Shreya Singhal v. Union of India, 2015 (5) SCC 1.

any new regulation of artificial or fake media must be carefully drafted in order not to repeat the constitutional pitfalls found in Section 66A, otherwise, satirical or artistic expression could be prohibited. On the other hand, following the procedural requirement of "actual knowledge" under Section 79 will render enforcement ineffective to combat the rapid spread of viral deepfakes during election cycles.

B. ELECTORAL LAW: REPRESENTATION OF THE PEOPLE ACT AND ELECTION COMMISSION

The RPA is still the foundation of Indian electoral legislation. Section 123(4) defines a corrupt practice as the publication of false statements about the personal character or conduct of candidates.[26] On the same note, Section 175 of the BNS[27] punishes false statements that relate to elections. One might think that such provisions can be applied to deepfake campaigns. Nevertheless, they assume a traditional form of publication, i.e., pamphlets, speeches, or newspaper advertisements. They remain quiet when it comes to digital disinformation and certainly when it comes to AI-generated forgeries.

In addition, prosecution under such sections including Section 100(1)(b) of the Act is tedious. Conviction needs to show that the candidate who benefited from the falsehood either knew it or consented to it, and prove that it materially influenced the outcome of the elections.[28] The same

---

[26] The Representation of the People Act, 1951, § 123(4).
[27] The Bharatiya Nyaya Sanhita, 2023, § 175.
[28] The Representation of the People Act, 1951, § 100(1)(b).

was discussed by the apex court in *Manohar Joshi v. Nitin Bhaurao Patil & Anr.*[29] With viral deepfakes that are anonymously distributed on social media, these evidentiary burdens are almost impenetrable.

The ECI is authorized and charged constitutionally by Article 324,[30] to conduct free and fair elections in the country, and has identified the severity of deepfakes. As discussed in the earlier analysis of the 2024 elections. The ECI Advisory circulars have the same structural shortcoming noted in the previous analysis because it operates under the MCC which is not a law.[31] Since the code relies primarily on moral persuasion rather than statutory authority, its enforcement mechanisms are limited to censures or temporary suspensions and remain ineffective against the sophisticated use of synthetic media. Therefore, the commission does not have legal authority to issue penalties or explicitly punish for disseminating deepfakes during election campaigns.

C. JUDICIAL APPROACH AND EVIDENTIARY ISSUES

In India, there has not yet been any judicial decision directly involving the use of deepfakes in elections. Nonetheless, applicable jurisprudence on digital evidence brings out the systemic problems. Supreme Court, in *Anvar P.V. v. P.K. Basheer,*[32] made it clear that electronic records could be accepted only through a certificate under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 ("**BSA**").[33] This position was

[29] Manohar Joshi v. Nitin Bhaurao Patil & Anr 1996 (1) SCC 169.
[30] INDIA CONST, art. 324.
[31] Election Commission of India Advisory Circulars, *supra* note 17.
[32] Anvar P.V. v. P.K. Basheer & Ors. (2014) 10 SCC 473.
[33] The Bharatiya Sakshya Adhiniyam, 2023, § 63.

further clarified by the Apex Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,*[34] which demonstrates the evidentiary difficulties in authenticating digital media. Here, it was held that the certificate is a condition precedent for the admissibility of electronic records, if the original device cannot be made available, while also recognizing the practical impossibility of acquiring such certificates from a third-party source such as any Social Media Platform. A further implication of this ruling is that a party can apply to the judiciary to produce a certificate from the appropriate authority. This procedure does create a legal avenue to produce certificates as evidence in court. Nevertheless, it does highlight the challenges relating to evidentiary value in relation to deepfakes. Where false information is disseminated virally, anonymously via encrypted platforms, identifying the origin or source of that content and obtaining a valid certificate poses an overwhelming forensic difficulty.

Deepfakes make it worse, even trained forensic analysis might not be able to conclusively prove manipulation, and in cases where manipulation detection technology is considerably less advanced than generative algorithms. In an election petition where the burden of proof is high on the petitioner, proving that a viral video was synthetic, malicious, and outcome-determinative would be very hard. Therefore, although the Indian law provides some elements of protection via BNS, IT Act, and RPA, none of them were created to protect against AI-manipulated

[34] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

content. What results is a patchwork regime: reactive, outdated, and inappropriate in addressing the special harms of electoral deepfakes.

IV. CONSTITUTIONAL DIMENSIONS

Deepfakes do not just reveal statutory lacunae, but rather involve constitutional values of the foundation. They bring into question the boundaries of freedom of speech, the right to privacy and their reputation, and the right of a voter to receive accurate information in a democracy. Indian constitutional jurisprudence can provide useful guideposts, and yet it is not clear that it can be applied to synthetic media.

A. THE INDEPENDENCE OF ELECTION AND THE FREEDOM OF SPEECH

Freedom of speech and expression is guaranteed under Article 19(1)(a) of Constitution.[35] Since the early instances, the Supreme Court has identified political speech as the key to democratic operation. In *Romesh Thappar v. The Court in the State of Madras,*[36] the court held free expression to be the basis of all democratic organisations. Similarly, in *Indian Express Newspapers (Bombay) v. In Union of India & Ors.,*[37] the Court opined that the press and political speech should be given the widest latitude in a democracy.

Nonetheless, Article 19(2)[38] permits reasonable restrictions, which can include the interests of defamation, public order, sovereignty, and

[35] INDIA CONST., *supra* note 7.
[36] Romesh Thappar, *supra* note 8.
[37] Indian Express Newspapers (Bombay) v. In Union of India & Ors., (1985) 1 SCC 641.
[38] INDIA CONST, art. 19, cl. 2.

integrity. In *Shreya Singhal v. Union of India,*[39]Section 66A of the IT Act was struck down as vague, but at the same time, the Court held that restrictions may be imposed provided they are narrowly tailored and are proportionate. This proportionality framework, even more systematized in *Modern Dental College v. State of Madhya Pradesh,*[40] the Supreme Court established that any restriction must be aimed at a legitimate end, must be appropriate to fulfil it, must be the least restrictive alternative, and must be balanced between rights and interests.

It is obvious when applied to deepfakes. Electronic media that is maliciously generated by synthesizing the speech of a candidate clearly destroys the electoral integrity and public order. At the same time, blanket bans on AI-generated content would ban legitimate campaign innovation, satire and parody. There must therefore be a balance between criminalizing deceptive deepfakes that aim to deceive the voters and leaving a space to allow protected political speech.

B. ARTICLE 21 RIGHT TO REPUTATION AND PRIVACY

Article 21 of the Constitution guarantees the right to life and personal liberty has been broadly interpreted to include dignity, reputation and privacy[41]. In *Board of Trustees of the Port of Bombay v. Dilipkumar Nadkarni,*[42]

---

[39] Shreya Singhal, *supra* note 25.
[40] Modern Dental College & Res. Cen. & Ors. v. State of Madhya Pradesh & Ors., (2016) 7 SCC 353.
[41] INDIA CONST, *supra* note 7, art. 21.
[42] Board of Trustees of the Port of Bombay v. Dilipkumar Raghavendranath Nadkarni, (1983) 1 SCC 124.

the Court said that "reputation is a part of personal security and is guarded under the Constitution." This was confirmed once again in *Subramanian Swamy v. Union of India,*[43] in which the Court affirmed criminal defamation laws by acknowledging reputation as an inseparable component of the right to life.

Deepfakes create a direct attack on this right. The production of a fake video with a candidate uttering disparaging statements can permanently damage an image, more so in the condensed period of an election campaign. Reputational harm is more urgent and irreversible than defamation in print; it can be refuted by corrective publications. The visceral effect of audiovisual deepfakes cannot be rebutted, and reputational harm is more imminent.

The concept of Privacy has also been lifted at the constitutional level. In *K.S. Puttaswamy v. Union of India,*[44] a nine-judge bench held that privacy is inherent to dignity and liberty. The judgment was focused on informational autonomy, the possibility of people having rights over the use of their personal information and identity indicators. Deepfakes as a form of manipulating biometric identifiers, including facial features and voice, without consent, are a direct infringement of this autonomy. The analogy is powerful here, as unauthorized surveillance has similarly infringed on privacy in the same way that unauthorized duplication of identity digitally is used to manipulate elections.

[43] Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
[44] Puttaswamy, *supra* note 9.

C. THE INFORMED CHOICE AND THE RIGHT TO KNOW OF THE VOTER

The Constitution conceives democracy on the basis of free and fair elections, which have been held to be a part of the basic structure by the apex court in *Indira Nehru Gandhi v. Raj Narain.*[45] Moreover, in *Union of India v. Association for Democratic Reforms,*[46] the Court declared that the voters have an inalienable right tao know the antecedents of candidates, as a result of Article 19(1)(a) of the Constitution. This principle was further upheld in *People's Union of Civil Liberties v. Union of India*[47] the Court had directed that criminal history and asset declarations of candidates should be disclosed.

Electoral deepfakes are a violation of the right to know. The moment voters are subjected to doctored speeches or untrue promises, their capacity to vote with informed choice is compromised. The damage in this case is that of collective, not individual harm. Reputational injury is certainly a harm to the candidate, but deepfakes also damage the information environment required to participate in a democracy. The analogy in *PUCL v. Union of India,*[48] in which the Court invalidated the voter

[45] Indira Nehru Gandhi v. Shri Raj Narain & Anr., (1975) 2 SCC 159).
[46] Union of India v. Association for Democratic Reforms, (2002) 5 SCC 294; *see also* Anushri Joshi, *Union of India v. Association for Democratic Reforms,* Association for Democratic Reforms, (Dec. 11, 2024), https://adrindia.org/content/article-18752-the-landmark-case-of-union-of-india-v-s-association-for-democratic-reforms-2002-5-scc-294-an-analysis-of-electoral-transparency-in-indian-democracy.
[47] People's Union of Civil Liberties v. Union of India & Anr., (2003) 4 SCC 399.
[48] People's Union of Civil Liberties & Anr. v. Union of India & Anr., (2013) 10 SCC 1; Harsheen Luthra & Aditya Ojha, *PUCL v. Union Of India: An Analysis Of The Impact Of NOTA,* Mondaq (Jun. 21, 2024), https://www.mondaq.com/india/court-procedure/1481972/pucl-v-union-of-india-an-analysis-of-the-impact-of-nota.

autonomy by maintaining a suitable option of none of the above ("**NOTA**"). In the same way that depriving people of accurate options impairs the process of choice, drowning the electoral arena with artificial lies spoils the process of decision-making.

In conclusion, these tensions can be solved within the framework of Indian jurisprudence. In the *Puttaswamy case*[49] and the *Modern Dental College case,*[50] the Court took the proportionality test as the criterion of assessment of limitations on fundamental rights. When applied to deepfakes, it implies that safeguarding electoral integrity and reputation/privacy protection, targeted regulation of deceptive deepfakes is an effective means to that end, watermarking and disclaimers should be favoured alternatives to an outright prohibition, and the damage to electoral democracy should be found to outweigh the curtailment of speech. Therefore, the Constitution does not require a two-option decision of either free speech or regulation. However, a straightforward ban on technology is also not the solution. Instead, the situation needs a standardized response that mitigates manipulation of elections without hindering legitimate political discourse.

V. COMPARATIVE INTERNATIONAL APPROACHES

The threat of deepfakes interference in the democratic process of elections is a global problem and therefore many countries are trying to find ways to regulate it in order to protect their citizens from harm. Each country has a very different approach due to their own respective political,

[49] Puttaswamy, *supra* note 9.
[50] Modern Dental College, *supra* note 40.

demographic, and legal conditions. Therefore, it is necessary for India to study the various approaches taken by other countries in order to develop a comprehensive regulatory scheme. For this purpose, this part analyses four countries as examples of their differing approaches which includes the European Union, United States, China, and Australia.

The first approach is the EU's compliance-based regulation, which focuses on evaluating risk rather than simply prohibiting access, the second is the US's restricted use of criminalization, the third is China's technology-based statutory requirements, and the fourth is Australia's collaborative self-regulatory systems. The objective of this analysis is to provide examples of regulatory mechanisms that can be adapted and integrated into India's regulatory framework and provide examples of how the functional components of other countries' laws could be combined to help protect India's democratic principles while still providing individual constitutional liberties.

A. WORLDWIDE ELECTORAL DEEPFAKE SPREAD

The Indian example falls into a general world trend. During the parliamentary elections in Slovakia in 2023, an AI-produced audio recording of the leaders of the opposition talking about vote manipulation was published a few days before the elections, and it is claimed that it affected the outcome of the elections.[51] Deepfake campaign videos have

[51] Morgan Meaker, *Slovakia's Election Deepfakes Show AI is a Danger to Democracy*, WIRED (Oct. 3, 2023), https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/.

been circulated by candidates in the United States of both Republican and Democratic parties, leading states like Texas and California to enact laws against such election-related deepfakes during specified campaign periods.[52] The European Union also forecasted such dangers and at the same time enlisted deepfakes among the highly risky AI in the scope of their Artificial Intelligence Act, which demands transparency, labelling, and responsibility of the platforms.[53] China takes this even further with its Deep Synthesis Regulations 2022 to require real-name verification of all AI-generated content creators and force an obvious watermarking of synthetic media.[54]

These instances indicate the fact that the electoral deepfakes are not unique or forward-looking. They are an immediate and cross-border threat to democracies around the globe. When other jurisdictions are setting out to experiment with specific legal solutions, India continues to be dependent on generic criminal law, intermediary liability regulation, and advisory practices. The dangers that have been revealed in the 2024 elections are likely to be multiplied before the next elections unless a specific regulation system is introduced.

---

[52] Sophie Loewenstein, Make America Fake Again?: Banning Deepfake Federal Candidates in Political Advertisements Under the First Amendment, 93 FORDHAM L. REV., at 273 (2024), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=6109&context=flr; Tex. Elec. Code Ann. § 255.004; Cal. Elec. Code § 20010.

[53] Mateusz Labuz, *Regulating Deep Fakes in the Artificial Intelligence Act*, 2 APPLIED CYBER SECURITY & INTERNET GOVERNANCE, (2023), https://doi.org/10.60097/ACIG/162856.

[54] Rogier Creemers & Graham Webster, *Translation: Internet Information Service Deep Synthesis Management Provisions (Draft for Comment)*, DIGICHINA (Feb. 4, 2022), https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/.

B. EUROPEAN UNION: TRANSPARENCY AND PLATFORM RESPONSIBILITY

The European Union has been in the lead in regulating artificial intelligence, with a horizontal strategy, which is, the EU Artificial Intelligence Act ("**AI Act**"). The AI Act has defined deepfakes as highly dangerous AI applications, and any AI-created or manipulated content must be prominently marked as artificial.[55] Moreover, the Digital Services Act, 2022 ("**DSA**"),[56] puts the duty on online platforms to detect and take down disinformation, including deepfakes, within very limited periods of time.

The European Commission, in particular, has sounded the alarm of possible deepfake threats to future parliamentary elections and reinforced the need to utilize watermarking technologies and hold platforms more accountable. One of the most important aspects of the model of the EU is that the responsibility is shifted to the platforms instead of individual victims or regulators.[57] The EU seeks to pre-emptively stop electoral deepfakes through its requirement of ex ante obligations, i.e., labelling and

---

[55] AI Act, *supra* note 4, art. 3(60).

[56] Regulation (EU) 2022/2065 of the European Parliament and of the Council, 19 Oct. 2022, A Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022, O.J. (L 277) 1.

[57] Andrea Bertolini et al., *Liability of Online platforms*, Panel for the Future of Science and Technology, Scientific Foresight Unit, European Parliamentary Research Service, European Parliament, PE 656.318, (Feb, 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf.

detection.[58] Although critics warn of excesses of regulation, the EU model shows an active spirit of ensuring electoral integrity without compromising on the freedom of democracy.

C. UNITED STATES: CRIMINALISATION AT THE STATE LEVEL

The United States does not have a broad federal law on deepfakes, although some states have already passed special laws, such as those in Texas and California. Texas bans the making and posting of deepfake videos to the extent of causing harm to a candidate or affecting the electorate, with a view towards the 30 days before an election.[59] California also follows a similar path and outlaws the distribution of deceptive audio-visual material in connection with an election campaign without a disclaimer.[60]

What makes these laws interesting is the fact that they are time-limited: the restrictions are permitted only during the sensitive phase just before elections, which is why the freedom of speech is balanced with the integrity of the elections. Enforcement is, however, not easy. Practically, harmful content may become viral until the time that law enforcement can

---

[58] Maurao Fragale & Valentina Grilli, *Deepfake, Deep Trouble: The European AI Act and the Fight against AI-Generated Misinformation*, COLUM. J.EUR. L. (Nov. 11, 2024), https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/.

[59] Tex. Elec. Code Ann., *supra* note 52, § 255.004; N. David Bleisch, *Deepfakes and American Elections*, American Bar Association (May. 6, 2024), https://www.americanbar.org/groups/public_interest/election_law/american-democracy/our-work/deepfakes-american-elections/.

[60] Cal. Elec. Code Ann., *supra* note 52, § 20010; Stuard D. Levi & Tyler Rosen et al., *California Elects New Laws to Combat AI Generated Deceptive Election Content*, Skadden, Arps, Slate Meagher & Flom LLP and Affiliates (Sept. 27, 2024), https://www.skadden.com/insights/publications/2024/09/california-enacts-new-laws.

identify and punish. In addition, First Amendment law subjects the regulation of speech to strict scrutiny, making it legally problematic. Nevertheless, the American experiment shows that criminalization can be narrowly focused, limited in scope to a specific time when elections are to be held, and acts as an example of democracies that are cautious of other forms of control.

D. CHINA: MANDATORY WATERMARKING AND REAL-NAME VERIFICATION

China has taken the most draconian route in the form of its Provisions on the Administration of Deep Synthesis Internet Information Services, commonly referred to as the Deep Synthesis Regulations.[61] According to these regulations, all AI-generated material must be labelled, and providers of the services must confirm the true identities of the users. Platforms must attempt to inhibit the spread of dangerous deepfakes, and non-compliance is punishable. Although this is a good way to prevent the spread of manipulated media, the Chinese strategy leads to the suspicion of too much state control and censorship. The model indicates an authoritarian philosophy of regulation, in which the state prescribes how the technology may be used. However, in functional terms, the Chinese system provides an example of the usefulness of mandatory watermarking

[61] Zhang & Laney, *China: Provisions on Deep Synthesis Technology Enter into Effect*, Library of Congress (Apr. 25, 2023), https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/; James Gong, *China to Strengthen Generative AI Regulation*, Bird & Bird (Jul. 03, 2024), https://www.twobirds.com/en/insights/2023/china/china-to-strengthen-generative-ai-regulation.

and ex-ante regulation of deepfake harms. In the case of India, which is a country that exists under a constitutional democracy, wholesale adoption of such stringent measures may be neither possible nor advisable. Nonetheless, factors like the need to implement labels and active platform responsibilities provide great insights.

E. AUSTRALIA: INTEGRITY AND DISINFORMATION CODES OF ELECTORAL CONDUCT

Australia has countered the deepfake challenge with a combination of self-regulation and electoral regulation. AEC has recognized the dangers of synthetic media and collaborates with technology platforms to identify and overcome election-related disinformation. In June 2023, the federal government launched a Discussion Paper on Safe and responsible AI in Australia, which identified the risks of deepfakes which can cause influence to the democratic processes or cause other deceit.[62]

In July 2024, Australia has also launched latest version of Australian Code of Practice on Disinformation and Misinformation (**"ACPDM"**), a voluntary code of conduct of the platforms such as Google, Meta, and TikTok, which contains promises to curtail the proliferation of misinformation, including deepfakes.[63] Although the code is not a legally binding document, it determines the requirement of reporting as well as the

---

[62] Dept. of Indus., Sci. & Res., *Safe and Responsible AI in Australia: Discussion Paper* (June 2023), https://consult.industry.gov.au/supporting-responsible-ai.

[63] Digital Industry Group Inc., *Australian Code of Practice on Disinformation and Misinformation* (Jul. 24, 2024), https://digi.org.au/disinformation-code/; Australian Communications and Media Authority, *Digital Platforms' Efforts under the Australian Code of Practice on Disinformation and Misinformation* (Jul., 2024), https://www.acma.gov.au/sites/default/files/2023-07/Digital%20platforms%20efforts%20under%20Code%20of%20Practice%20on%20Disinformation%20and%20Misinformation.pdf.

transparency requirement. The critics reason that the use of self-regulation might not be enough; however, the cooperative model has developed a system of accountability that did not enable direct legislative intervention.

Australian experience with deepfakes and AI content shows that co-regulation has potential in which government agencies work together with platforms within a framework, but with a flexible code. In the case of India, this strategy provides ideas on how to balance the state intervention and the role of the private sector in the context of the size of social media platforms present in India.

F. LESSONS FOR INDIA

In conclusion, there are four comparative regulatory strategies as noted above, which are the EU's ex ante platform obligations,[64] the United States' narrowly-drawn criminalization during elections,[65] China's mandatory labelling and real-name verification,[66] Industry codes co-regulation in Australia.[67] They all are products of the political spirit of their jurisdiction, European preventive governments, American constitutional hesitation, Chinese authoritarian governance, and Australian collaborative governance. For India, a hybrid regulatory approach that incorporates international best practices in a unique configuration tailored to meet

[64] EU Artificial Intelligence Act, art. 3(60); DSA, *supra* note 56; Bertolini et al., *supra* note 57; Fragale & Grilli, *supra* note 58.
[65] Tex. Elec. Code Ann. & Bleisch, *supra* note 59; Cal. Elec. Code & Levi Rosen, *supra* note 60.
[66] Zhang & Gong, *supra* note 61.
[67] Dept. of Indus., *supra* note 62; Digital Indus. Grp. Inc. & ACMA, *supra* note 63.

India's specific demographic and political landscape would be highly efficient. This approach will be based upon four key elements.

Firstly, the implementation of the EU's transparency mandate through machine-readable labeling of synthetic contents that empowers India's linguistically diverse electorate to identify and distinguish such contents. Secondly, the establishment of temporary restrictions of deceptive deepfakes similar to state law in the US during a pre-election period so that voters cannot be influenced by disinformation that cannot be verified just before an election. Thirdly, the model should incorporate China's provenance protocols that mandates watermarks for deceptive contents and encrypted distribution services to the platforms like WhatsApp so that the malicious content can be traced back to its source. Lastly, the establishment of a co-regulatory framework similar to Australia's that will provide for a compliance structure of digital intermediaries establishing a co-ordinated relationship between the ECI and digital intermediaries for proactive detection. By adapting these mechanisms to accommodate and consider each country's local constitutional realities, this framework meets the proportionality test established by Article 19(2) of the Constitution, thus promoting the protection of the integrity of elections while upholding the rights of individuals without interfering with their freedom of expression.

VI. IDENTIFICATION OF GAPS AND RECOMMENDATIONS

A. LACUNAS IN THE PRESENT LEGAL SYSTEM

The 2024 elections have shown one thing undoubtedly: India needs to overhaul its existing legal framework to handle the peculiarities of deepfakes. Although defamation, forgery, obscenity, or identity theft are crimes criminalized by general clauses contained in the BNS, and the IT Act, none of them directly consider synthetic media as a distinct type of harm. The RPA, which was framed when the world was not digitally oriented, is also obsolete. Even the clauses like Section 123(4) that penalize false statements of candidates assume the presence of human agency and customary forms of campaigning.[68] Practically, this provision can hardly be applied to viral deepfakes, as it needs to prove intent, authorship, and, at the same time, having a direct effect on the electoral outcome, which is virtually impossible in the disordered information sphere of social media.

ECI, which is one of the most trusted constitutional bodies in India, is currently limited to advisory and model code of conduct enforcement. It lacks the legal authority as well as the technological platform to take action effectively in cases where manipulated information goes viral on the Internet. That places the integrity of elections squarely on the voluntary adherence of political actors and vehicles. There is also a challenge with judicial institutions. The authentication of electronic evidence under Section 63 of the BSA, 2023,[69] has always been a problematic issue, as seen

[68] Representation of the People Act, *supra* note 26.
[69] Bharatiya Sakshya Adhiniyam, *supra* note 33.

in *Anvar P.V.'s case*[70] and *Arjun Panditrao's case,*[71] in which the Court demanded strict certification. The evidentiary obstacles in this context become particularly dangerous given the setting of deepfakes, in which the question is whether evidence takes place or not, because digital fiction is the very premise of the matter.

B. REFORM SUGGESTIONS

The solution to these gaps lies in reforms at various levels, e.g., legal, institutional, technological, and civic. The aim of the reform agenda should not be to gag political expression and innovation, but rather to ensure fairness in the process of electing leaders and that voters are not deceived by misconduct or manipulations.

The legal system requires a statutory solution at the level of expressly recognizing deepfakes in Indian law. Representation of People Act needs to be amended and criminalize the use of AI-generated content that is aimed at deceiving voters or distorting the discourse around elections. This would align electoral law with modern-day digital realities. In the same vein, the BNS may consider a more specific criminal offence of malicious synthetic impersonation, which is an offence that focuses on content that is generated in an attempt to mislead without the consent of the parties and with the intent to mislead. Notably, these provisions should be well designed to avoid satire, parody, authorised AI usage, and lawful political speech and, therefore, meet the demands of Article 19.

---

[70] Anvar P.V., *supra* note 32.
[71] Arjun Panditrao, *supra* note 34.

Institutionally, the Election Commission should be fortified. It must not be confined to mere issuance of advisories but ought to be given the statutory powers by the Parliament to monitor, investigate and punish the misuse of deepfakes in campaigns. An expert team of the ECI, composed of AI specialists, forensic investigators, and lawyers, would allow the quick identification and reaction to synthetic information through a dedicated section, the so-called Digital Integrity Cell. This model would sustain the independence of the Commission, and also prepare it to face the challenges of the twenty-first century.

Even platforms should be held responsible. India should also consider adopting a co-regulatory regime, taking cues for the same globally, in which platforms will be required to label or watermark AI-generated content, give users a clear disclaimer, and create quick response mechanisms to tackle misinformation during election time. The ECI would be able to provide oversight, which would make the approach accountable but still leave it to industry experts to work out the details of how it would operate. This kind of framework is a middle ground between the two extremes of heavy state censorship and laissez-faire. It is also important to reform the judicial and evidentiary issues. The standards of forensic certification of AI-created content should be included in section 63 of the BSA. Technical support is needed in courts so that they can establish the authenticity of a piece of digital evidence or whether it has been manipulated or not. Unless there are such reforms, the prosecution of any newly established offence will be merely symbolic.

Last but not least, a sustainable solution is built on civic resilience. Regardless of how strong laws and technologies develop, deepfakes will keep on developing. It is thus imperative to have a paralleled approach to educate the voters. Media literacy campaigns, as organized on the scale of the successful SVEEP programme,[72] run by ECI, can provide citizens with the tools to doubt, countercheck, and critically evaluate online material. Regulation is not paternalistic but helps to create a democratic culture that cannot be manipulated by voters because they are empowered.

C. BALANCED INDIAN MODEL

Useful lessons are provided by comparative experience. Europe has been working on proactive platform duties, detection, labelling, and risk assessment obligations in the DSA and the AI Act.[73] Although the United States is more hesitant about the ban on free speech, deepfakes that mislead voters in certain states and at certain stages of the campaign have been criminalized.[74] China has gone even further and requires real-name registration of creators and forced watermarking of all AI-generated materials, with severe punishments[75]. Australia has favoured a co-regulatory approach, in which the platforms themselves make voluntary promises to meet standards of detection and transparency, watched over by regulators[76].

---

[72] Election Commission of India & U.N. Dev. Programme, *Systematic Voters' Education & Electoral Participation (SVEEP)* (2024), https://www.undp.org/sites/g/files/zskgke326/files/migration/in/SVEEP.pdf.

[73] EU Artificial Intelligence Act, art. 3(60); DSA, *supra* note 56; Bertolini et al., *supra* note 57; Fragale & Grilli, *supra* note 58.

[74] Tex. Elec. Code Ann. & Bleisch, *supra* note 59; Cal. Elec. Code & Levi Rosen, *supra* note 60.

[75] Zhang & Gong, *supra* note 61.

[76] Dept. of Indus., *supra* note 62; Digital Indus. Grp. Inc. & ACMA, *supra* note 63.

India must not simply copy-paste all these rules in order to change them. Its political culture, electoral scope and constitutional structure are different from the above-mentioned countries. Instead, India can use a hybrid approach combining the international best practices and local realities. This kind of model would ensure that the only deepfakes criminalized are malicious ones and that reputation and privacy are not infringed on at the expense of satire and political creativity. It would grant the ECI specific supervisory authority, which would be independent and unbiased in application. It would also put strict requirements on platforms to tag and identify synthetic material, but not too much censorship or monitoring. Courts would be modernized to include evidence standards adjusted to the problems of AI, and citizens themselves would be prepared through literacy campaigns to be able to operate in the digital information space.

In conclusion, the Indian reaction cannot be a hammer but a finely balanced structure, that is, it protects against manipulation but reaffirms the constitutional promise of free expression, dignity, and informed choice. This type of model would not only help to solve the current issue of electoral deepfakes but also create a pattern of how democracies should deal with disruptive technologies without jeopardizing their own values.

VII. CONCLUSION

Deepfakes are not only a technological abnormality but a threat to electoral democracy per se. Their application in the 2024 elections showed

how simple it is to manipulate political speech through synthetic content, confuse voters, and undermine the trust in institutions. The current system in India, based on old laws, weak positions of the Election Commission, and defences to platform liability, is one that is literally ill-equipped to deal with this issue.

The answer is not mass censorship but common-sense regulation. Democracy can be preserved through proportionate reform, which does not ruin or affect creativity. Changes to the law on elections should be one that bans malicious synthetic impersonation, with satire and parody still being covered. The Election Commission must also have statutory powers and technical knowledge via a special Digital Integrity Cell. A co-regulatory system should be established that gives platforms the responsibility to label and quickly take down misleading content, and also allows the industry to be innovative. Courts should also modernize the evidence rules in order to cope with the manipulation based on AI. And most importantly, the citizens themselves should be empowered by means of voter education and media literacy. There is no technological protection that can be effective without the ability of the voters to challenge and check what they are consuming.

In this regard, the control of deepfakes should not be considered an attempt to censor speech but rather a means to maintain informed consent, which is the pillar of democracy. India can use a firm but proportionate framework to turn the deepfake crisis into an opportunity to reinforce and reaffirm constitutional values, safeguard electoral integrity,

and be a model to other democracies around the world going through the digital age.

NLUJ Law Review

Sumati Arora, *Comparative Analysis of Fraud Prevention in RBI's Payment Aggregator Directions and the EU's PSD3 Framework,* 12(1) NLUJ L. REV. 76 (2026)

COMPARATIVE ANALYSIS OF FRAUD PREVENTION IN RBI'S PAYMENT AGGREGATOR DIRECTIONS AND THE EU's PSD3 FRAMEWORK

~ *Sumati Arora*[*]

ABSTRACT

*This article analyses the current regulatory framework on prevention of fraud for Payment Aggregators ("**PAs**") in India. It identifies key gaps in the Reserve Bank of India's ("**RBI**") (Regulation of Payment Aggregators) Directions, 2025, particularly concerning their limited effectiveness in addressing sophisticated frauds such as spoofing and social engineering attacks. The article highlights how current regulatory models in India rely heavily on Know Your Customer ("**KYC**") and merchant onboarding requirements and fail to impose clear responsibilities on PAs. The article employs doctrinal research to examine statutory frameworks, circulars, and case laws in order to assess the current framework. The research finds that implementation by PAs remains inconsistent, with liability for fraud-related losses often ambiguously assigned and shifted onto merchants or financial institutions. Further, the amended Directions suggest a contractual based liability regime than affixing liability on actual point of failure. In contrast, the European Union's ("**EU**") Payment Services Directive 3 ("**PSD3**") framework provides a more cohesive model, offering clearer liability rules and advanced*

[*] Sumati Arora is a fourth-year student pursuing B.Sc. LL.B. (Hons.) (Cyber Security) at National Law Institute University, Bhopal.

*fraud mitigation tools. The article compares the Indian and the EU framework concluding with practical recommendations for regulatory reform in India, including the adoption of account name-verification mechanisms akin to Europe's International Bank Account Number ("**IBAN**"), name matching, expansion of consumer protection frameworks to cover social engineering fraud, and exploring a negative database for flagged transactions. These recommendations aim to strengthen security obligations across stakeholders, and enhance consumer trust in digital payments.*

TABLE OF CONTENTS

I. INTRODUCTION 79
II. CURRENT REGULATORY FRAMEWORK FOR PA AND PGS IN INDIA.....82
A. LEGAL IMPLICATIONS OF CLASSIFICATION AS PAYMENT AGGREGATORS AND PAYMENT GATEWAYS 83
III. REQUIREMENTS FOR PREVENTION OF FRAUD 86
A. DATA STORAGE LIMITATIONS 86
B. MERCHANT ONBOARDING STANDARDS 87
C. IMPLEMENTATION OF FRAUD PREVENTION REQUIREMENTS.....90
IV. LACUNAE IN THE FRAUD PREVENTION REQUIREMENTS 91
V. THE EUROPEAN FRAMEWORK ON FRAUD PREVENTION 95
VI. SUGGESTIONS FOR STRENGTHENING FRAUD PREVENTION POLICIES OF INDIA IN DIGITAL PAYMENTS ECOSYSTEM 97
A. ENHANCING ACCOUNT VERIFICATION MECHANISMS 97
B. ASSIGNING LIABILITY AND STRENGTHENING PAYMENT AGGREGATOR ACCOUNTABILITY 99
C. EXPANDING CONSUMER PROTECTION AGAINST SOCIAL ENGINEERING FRAUDS 99
VII. CONCLUSION.....100

I. INTRODUCTION

The payment industry has witnessed a significant transformation, moving from barter systems to using money as a medium of exchange and now to digital payment methods. This change, driven by technology, has changed how financial transactions work, making them more convenient for both consumers and businesses. The Digital payment ecosystem of India includes several intermediaries that facilitate the transactions and work on various levels such as settling, handling and processing funds.

At the forefront of this transformation are PAs and Payment Gateways ("**PGs**"), which serve as intermediaries between consumers and merchants. PAs are entities responsible for onboarding merchants, facilitating transactions, and settling payments on behalf of customers in exchange for goods and services.[1] These transactions can be conducted online or through physical points of sale integrated with the merchant's interface. On the other hand, PGs are not involved in the handling of funds, and these entities merely provide technology infrastructure for routing and facilitating online transactions.[2]

The Discussion Paper on Payment Aggregators by RBI ("**the Discussion Paper**") highlighted that the customers had limited ways to seek redress from such aggregators, i.e., only by way of the merchants or

---

[1] Aron Varghese, *Regulation of Payment Gateways and Payment Aggregators under the Payment and Settlement Systems (PSS) Act: Legal Framework and Challenges*, 7 INDIAN J.L. & LEGAL RSCH. 3177 (2024).
[2] *Id.*

banks.[3] In light of this, the Discussion Paper suggested regulation of such aggregators by enacting the Payment Systems Settlement Act, 2007 ("**PSS Act**"), which remains the primary legislation governing payment settlement systems in the country.[4]

The RBI issued Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020 ("**the Guidelines**") under Section 18 read with Section 10(2) of the PSS Act for regulation of the PAs. However, despite these provisions, the customers and merchants are still exposed to risks such as fraud, security breaches, and money laundering. Recently, in response to incidents of fraud and siphoning of funds, the Indian Cybercrime Coordination Centre ("**IC4**") released an advisory to address the frauds committed using mule accounts.[5] One such case of fraud, resulting from a vulnerability in the system of Safexpay Technology Pvt. Ltd., was reported in Thane, Maharashtra.[6] This later unravelled the extensive siphoning of funds involving huge transactions to foreign parties. In response, the RBI introduced the Financial Fraud Risk Indicator ("**FRI**") in July 2025, under the Digital Intelligence Platform to strengthen

[3] Reserve Bank Of India, *Discussion Paper on Payment Aggregators and Payment Gateways* (May 18, 2024), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DPSSDISCUSSIONPAPEREFCF5B7E17F9431185BD4FD57E540F47.PDF.

[4] The Payment and Settlement Systems Act, No. 51 of 2007 (India).

[5] Press Information Bureau, *RBI Advises Banks to Integrate FRI to Prevent Financial Frauds*, PIB (July 24, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2069000.

[6] Anamika Gharat, *Accused Who Hacked into Payment Gateway and Stole ₹25 Crore Booked*, HINDUSTAN TIMES, (Oct. 9, 2023, 8:00 AM), https://www.hindustantimes.com/cities/mumbai-news/accused-who-hacked-into-payment-gateway-and-stole-25-crore-booked-101696792286024.html.

cyber protection by categorising mobile numbers based on fraud risk.[7] Subsequently, the Guidelines were superseded by Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025 ("**the Directions**") on 15 September, 2025.[8]

In this backdrop, the article identifies the lacunae in the Directions along with other related ancillary regulations. It examines the changed landscape vis-à-vis the issues such as ineffective implementation of these guidelines by PAs and the effectiveness of liability regime in cases of fraud. Moreover, the Directions fail to adequately address specific risks, such as spoofing and impersonation frauds, leaving comprehensive KYC procedures and merchant onboarding norms for PAs as the sole framework to rely on to address these frauds. The article then analyses the requirements such as merchant KYC, data storage restrictions, and real-time fraud detection mechanisms. [9]

To address the identified lacunae, this article suggests adopting a framework similar to the Third Payment System Directive ("**PSD3**") of the European Union with respect to fraud prevention and proposes recommendations to strengthen the Indian regulatory environment.

---

[7] Editorial, *RBI Advises Banks to Integrate DoT's Financial Fraud Technology*, ECONOMIC TIMES (July 2, 2025, 09:18 PM), https://economictimes.indiatimes.com/industry/banking/finance/banking/rbi-advises-banks-to-integrate-dots-financial-fraud-technology/articleshow/122209879.cms.

[8] Reserve Bank of India, *Master Direction on Regulation of Payment Aggregators* (PA), RBI/DPSS/2025-26/141, CO.DPSS.POLC.No.S-633/02-14-008/2025-26 (Sept. 15, 2025), https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12896.

[9] Reserve Bank of India, *Guidelines on Regulation of Payment Aggregators and Payment Gateways*, RBI/2020-21/117 (Mar. 17, 2020).

II. CURRENT REGULATORY FRAMEWORK FOR PA AND PGS IN INDIA

The "Payment System" involves all the entities, software, technology and methods enabling payment between a payee and beneficiary. Further, Section 25 of the PSS Act authorises the RBI to regulate payment systems in India.[10] Using this authority, the RBI introduced the Guidelines in 2020, now superseded by the Directions.[11] The Directions were introduced after the introduction of the Draft Circular for Comments on Regulation of Payment Aggregators ("**Draft Circular**") on April 2024 by RBI along with the clarifications on the Guidelines to extend the scope of applicability and to enhance security and transparency.[12] The Directions establish a framework delineating the responsibility, rights and liabilities of PAs and gateways that have access to sensitive customer data and funds further, mandating continuous compliance. Further, the Directions consolidate regulations for PAs, including cross-border operations, rationalise definitions of categories of PAs, set out an authorisation regime, due diligence obligations, escrow account rules, etc. The Directions apply to both online PAs that facilitate transactions in non-Delivery-vs-payment transactions ("**DvP**") mode i.e., transactions where services are made available instantly on payment and

[10] The Payment and Settlement Systems Act, § 25, No. 51 of 2007 (India).
[11] Reserve Bank of India, *Regulation of Payment Aggregators (PAs) – Draft Directions,* Press Release No. 2024-2025/116 (Apr. 16, 2024), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=57713.
[12] Reserve Bank of India, *Regulation of Payment Aggregators (PAs)* – Draft, Circular for Comments, CO.DPSS.POLC.No.S-***/02-14-008/2024-25 (2024), https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=4419.

physical PAs which enable face-to-face payment for DvP transactions and cross-border PAs that facilitates foreign facilitates cross-border payments.[13] Furthermore, the Directions aims to provide clarity and financial stability by providing a risk management and customer protection framework aligning with the PSS Act and the Foreign Exchange Management Act, 1999 ("**FEMA**").

A. LEGAL IMPLICATIONS OF CLASSIFICATION AS PAYMENT AGGREGATORS AND PAYMENT GATEWAYS

Recently, in an incident involving Safexpay Pvt. Ltd., hackers breached the payment gateway of the company, changed its database, increased the wallet balances and using merchant credentials, they logged into the company's portal and carried out transactions to different bank accounts.[14] Under clause 9 of the Directions, PAs are required to adopt the baseline technology, i.e., information security governance that includes carrying out risk assessment of resources, identification of risks to security and ensuring overall compliance to secure Information Technology systems. However, these obligations do not apply to PGs that are only encouraged to follow the baseline technology.[15] This creates a regulatory gap that may be exploited by entities claiming the status of a PG while performing functions more aligned with that of a PA, thus drawing attention to the definition and scope of PAs and PGs.

---

[13] *Id.*
[14] *Supra* note 6.
[15] Payment Aggregators Guidelines, 2020, *supra* note 9, cl. 10.2.

The Directions defines PAs as entities facilitating digital transactions for e-commerce sites and merchants.[16] It acts as an interface connecting merchants with the banks and customers to receive payments from customers, pooling and subsequently transferring them to the merchants.[17] In contrast, PGs provide technology infrastructure to route and facilitate the processing of an online payment transaction without any involvement in the handling of funds.[18] This definition excluded the DvP transactions where delivery of goods or services and payment occur simultaneously. The Directions includes transactions processed via physical point of sale devices in the definition of PAs.

The definition and the scope of PA was further clarified in the case of *Hoichoi Technologies (P) Ltd. v. RBI,* decided by the Calcutta High Court.[19] In this case, Hoichoi Ltd., an entertainment company that is available on Google Play, filed a writ petition against RBI to consider expeditiously its complaint against Google Play for operating as a PA without authorisation under the PSS Act, 2007.

The court rejected the argument of petitioners to consider Google Play as a PA noting that the service fees charged by Google relate solely to the provision of platform-related facilities. These include hosting applications, enabling their visibility to users, and allowing downloads and purchases.[20] It was further observed that service charges were levied for

[16] Payment Aggregators Guidelines, 2020, *supra* note 9, cl. 1.
[17] Payment Aggregators Guidelines, 2020, *supra* note 9, cl. 1.1.1.
[18] Payment Aggregators Guidelines, 2020, *supra* note 9, cl. 1.1.2
[19] Hoichoi Technologies (P) Ltd. v. Reserve Bank of India, 2024 SCC OnLine Cal 3569.
[20] *Id.*

carrying products on the Google Play platform and are imposed when the platform is exploited for commercial purposes by the petitioners.

The High Court dismissed the petition holding that the entity can only be classified as PA if it is involved in the entire payment chain from "end-to-end." Merely facilitating e-commerce sites and merchants in accepting payment from the customer for completion of their payment obligations does not qualify a platform as PA. The role of PA is accepting, processing, and passing the money from the customers to the merchants.[21] In this case, Google Play Services only provided a platform for hosting developers and App operators to the online platforms. Further, the High Court found no evidence to show that Google Play handled payment settlement from merchants to customers to act as a PA.

Given the minimal distinction between the definitions of PAs and PGs, yet the significantly different compliance burdens they carry, entities may claim to operate as PGs while effectively functioning as PAs. Therefore, in light of this case, the role of Safexpay in collecting funds and ultimately settling them in the merchant's bank account must be carefully examined to determine its liability for failing to maintain adequate controls. Safexpay could argue that, as a payment gateway, it is not obligated to implement the baseline technologies mandated under the Directions to potentially absolve it of liability. However, if it is established that Safexpay operates as a PA and the breach was due to unsecure systems allowing the

[21] *Id.* at 19.

hackers to tamper with the database, then its obligation to comply with the prescribed Directions would be unequivocally proven, thereby affirming its liability.

III. REQUIREMENTS FOR PREVENTION OF FRAUD

Given the role of PAs in processing transactions and storing sensitive customer financial data, PAs are required to implement security, fraud prevention and risk management policies under the Directions.[22] RBI under the clause 9 of the Directions provides for fraud prevention and setting up a security, fraud prevention and risk management framework by laying down strict data storage, audit and implementation of baseline technologies requirements. Further, Chapter IV mandates KYC requirements for onboarding merchants in addition to ensuring mechanisms to monitor transactions by the merchants. The Directions also provide for assisted due-diligence of merchants for non-bank PAs.[23] A PA will need to undertake Contact Point Verification ("**CPV**") and duly verify the bank account in which the funds of small merchants are settled.[24]

A. DATA STORAGE LIMITATIONS

RBI mandates limiting the data storage with the PAs as a way of preventing fraud. Clause 4 of the RBI's Statement on Developmental and Regulatory Policies mandates that end-to-end payment and settlement

[22] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 9.
[23] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 13.
[25] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 13(b)(i); Ajinkya Kawale, *RBI Mandates Offline Payment Aggregators to Verify KYC for Merchants*, BUS. STANDARD (Apr. 17, 2024), https://www.business-standard.com/finance/news/rbi-mandates-offline-payment-aggregators-to-verify-kyc-for-merchants-124041700787_1.html.

information must only be stored by Payment System Operators ("**PSOs**"), which are entities facilitating payment between payer and beneficiary that includes clearing, payment settlement services etc.[25] PAs may retain limited data for fraud detection, such as identifying blacklisted entities, without storing customer account details.[26] The Directions are applicable to face-to-face or proximity payment transactions and bars all the entities involved in payment card transactions except card issuers and card networks from storing the card data.[27] Further, it mandates that any previously stored data should be purged.[28]

B. MERCHANT ONBOARDING STANDARDS

According to clause 9 of the Directions, PAs must ensure that the merchants they onboard comply with security standards like Payment Card Industry Data Security Standard and Payment Application Data Security Standard.[29] These standards help secure financial transactions and minimise fraud risks. Additionally, the framework prohibits PAs from storing customer financial data, except for minimal information necessary for transaction tracking. Such storage must comply with the "Storage of Payment System Data" circular released by RBI that is applicable to system

---

[26] Reserve Bank of India, *Statement on Developmental and Regulatory Policies*, cl. 4, (Feb. 05, 2021), https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=51078.
[27] Reserve Bank of India, *frequently asked questions - Storage of Payment System Data, FAQ 3* (2019) https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995.
[28] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 4(i).
[28] FAQ - Storage of Payment System Data, *supra* note 27, cl. 1.
[29] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 9; Payment Card Industry Security Standards Council, *Payment Card Industry Data Security Standard (PCI DSS)* v4.0 15 (Mar. 2022).

participants, service providers, intermediaries, payment gateways, third-party vendors, which allows storing transaction details like timestamps, transaction references, and system information but prohibits retaining account-related data only within India.[30]

Even though the Guidelines provided for storage of data for "limited purposes", it vested a greater discretion in the PAs to decide which data is necessary for transaction tracking purposes. The notified Directions amend this and PA provide clarity in laying down in strict terms the data that can be stored for transaction tracking or reconciliation purposes by PAs can only be the last four digits of the card number and the card issuer's name.[31]

Building upon these foundational requirements for merchant onboarding and the broader emphasis on strict KYC, the Guidelines further details the due diligence obligations of PAs.[32] These clarifications mandate that PAs conduct due diligence of merchants they onboard in accordance with the Customer Due Diligence requirements outlined in the Master Directions on KYC ("**MD-KYC**"), 2016.[33]

The detailed KYC verification under the Draft Circulars categorizes merchants into small and medium merchants, specifying varied degrees of due diligence based on the annual turnover, i.e., small merchants (turnover

---

[30] Storage of Payment System Data, *supra* note 27.
[31] Draft Regulation of Payment Aggregators, 2024, *supra* note 12, cl. 7.
[32] Draft Regulation of Payment Aggregators 2024, *supra* note 12, cl. 4.
[33] Reserve Bank of India, *Master Direction - Know Your Customer (KYC) Direction*, RBI/DBR/2015-16/18 (2016), https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607.

below INR 5 lakh) and not GST registered, must conduct CPV of the business establishment and verify the bank account where funds are settled and medium merchants (turnover below INR 40 lakh) and not GST registered, PAs are required to perform CPV and verify one Officially Valid Document ("**OVD**") such as a passport or Aadhaar number, etc., as defined under the MD-KYC of the proprietor or beneficial owner, along with the business.[34]

Furthermore, the Directions state that the assisted Video-based Customer Identification Process shall be allowed with the help of an agent at the merchant end, with PAs mandatorily maintaining records of the agent assisting the merchant.[35] PAs had to continuously monitor merchant transactions and migrate merchants to higher Customer Due Diligence categories based on transaction patterns, prescribing additional due diligence to be performed immediately upon such migration.[36] Finally, the Master Direction sets a firm transition timeline: PAs must ensure that merchants onboarded up to December 31, 2025 comply with the prescribed due-diligence requirements within one year from the date of the Master Direction; and from January 1, 2026 all newly onboarded merchants must be onboarded in accordance with the MD's due-diligence requirements.[37]

---

[34] *Id.*
[35] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 15.
[36] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 13(h).
[37] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 13(j).

C. IMPLEMENTATION OF FRAUD PREVENTION REQUIREMENTS

The Directions suggest a strong risk management system for PAs through Baseline Technology Recommendations for the prevention and detection of fraud. Non-bank payment system operators are required to deploy a real-time fraud monitoring system to identify suspicious transactional behaviour and generate alerts.[38] However, even though these recommendations are mandatory for PAs, they are merely suggestive for PGs, and the Directions do not establish any regulatory body to ensure strict compliance, creating a gap in enforcement.[39] While RBI oversees compliance and ensures adherence through audits and inspections by CERT-In empanelled auditors under the Cyber Resilience and Digital Payment Security Controls for Non-Bank PSOs,[40] other requirements like compliance with security standards like PCI-DSS and PCI-SSF and other baseline technology recommendations largely rely on self-regulation by PAs, leaving enforcement of these measures dependent on the PA's internal governance and reporting mechanisms.

The fraud prevention model adopted by Razorpay, a registered PA, serves as a representative example of how such entities address and manage fraudulent transactions.[41] If notified by a facility provider about

---

[38] Editorial, *RBI Issues Norms to Improve Safety of Payment Systems with Fraud Monitoring*, BUS. STANDARD (Mumbai, July 30, 2024), https://www.business-standard.com/finance/news/rbi-issues-norms-to-improve-safety-of-payment-systems-with-fraud-monitoring-124073001393_1.html.

[39] Vaishnavi P. & Ananya S., *An Assessment of the Liability of Payment Aggregators in India under the RBI Guidelines,* 1 CLCR 100 (2023).

[40] Reserve Bank of India, *Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators*, RBI/DPSS/2024-25/123, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12715.

[41] Razorpay, *Terms of Service* (Razorpay, undated), https://razorpay.com/terms/.

unauthorised debits, Razorpay can suspend merchant settlements while investigations are ongoing. Razorpay also addresses chargebacks, resolving them as per the agreed terms and applicable regulations. Notably, its liability is limited by disavowing responsibility for losses from fraudulent domestic or international transactions. It also places liability on merchants if they breach UPI fraud liability guidelines of the National Payments Corporation of India ("**NPCI**"), with the final decision in such cases resting with the concerned acquiring bank or NPCI.[42] These provisions allow PAs like Razorpay to reduce their exposure to fraud-related risks. They shift responsibility onto merchants, facility providers, and financial institutions, emphasising the need for rigorous compliance on all fronts.[43]

IV. LACUNAE IN THE FRAUD PREVENTION REQUIREMENTS

With the case of *PayPal Payments Private Limited v. Financial Intelligence Unit of India*, PayPal has been categorised as a registered entity under the Prevention of Money Laundering Act, 2002, which makes it obligated to follow the mandatory disclosure and Customer Due Diligence requirements.[44] This judgment has expanded the scope of obligations to be complied with by the payment systems; however, the practical implementation of the Directions by the PAs is in question. The policy of Razorpay and like platforms limits the direct involvement of PAs in

[42] *Id.*
[43] *Id.*
[44] Paypal Payments Private Limited v. Financial Intelligence Unit India and Ors., 2023 SCC OnLine Del 4336.

managing fraud-related losses of suspending settlements during investigations by placing reliance on acquiring banks and NPCI for dispute resolution. So, while fraud prevention policies for PA strengthen merchant accountability, they leave certain gaps in defining the liability of PA per se. For instance, the Razorpay model limits the role of PA primarily to ensuring compliance, while leaving the bulk of fraud prevention measures, such as transaction monitoring, with the merchant.[45]

The ambiguity in defining the liability of PAs becomes particularly problematic when fraud arises due to third-party faults. A notable example is the case involving the Australian retailer Stan Cash.[46] The payment portal was compromised by a third-party service provider, leading to a security breach that exposed sensitive customer information for an entire year. A customer suffered a loss of USD 6,000 in fraudulent transactions after making a purchase and the retailer attributed the breach to a third-party provider, leading to ambiguity in assigning liability when external entities are involved. This ambiguity has been addressed by the Directions as it requires the PA to have an agreement clearly delineating the roles and responsibilities of the parties involved i.e., the merchant, acquiring banks and other stakeholders.[47] The Directions also requires the PA to disclose

[45] Razorpay Terms of Service, *supra* note 41.
[46] Sarah Sharples, *Aussies $6k Card Fraud After Retailer's Payment Portal Hacked*, NEWS.COM.AU (Dec. 5, 2024), https://www.news.com.au/finance/money/costs/aussies-6k-card-fraud-after-retailers-payment-portal-hacked/news-story/bbda54842ef42326eebffc73842e1ccf.
[47] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 8(b).

comprehensive policies of merchant onboarding, privacy policy and other terms and conditions on website or mobile application.[48]

However, from the customer's perspective the enforcement still remains ambiguous due to the different interpretation of customer liability. Recently, the Allahabad High Court in *Suresh Chandra Singh Negi v. Bank of Baroda* court refused to hold the bank liable for the alleged third-party fraudulent transaction by the customers.[49] The court concluded that the transaction was conducted by the customers voluntarily and thus it will not be covered under the Clause 6(a) of the RBI circular of 2017 on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.[50] Clause 6(a) entitles customer to zero liability if the unauthorised transaction results from the negligence of bank or a third-party breach, provided it is reported in due time. In this case the court observed that the petitioners logged in to the bank accounts and OTP was generated on their registered number and the IP address and device data showed that the same system was used for the transaction so no third-party breach could be inferred. The court desisted to rely on the Supreme Court case of *State Bank of India v. Pallabh Bhowmick & Ors.* where the transactions relating to the customer's bank account were found to be unauthorised and the bank was held responsible for the same.[51] The decision was based on

---

[48] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, cl. 8(c).
[49] Suresh Chandra Singh Negi v. Bank of Baroda, 2025 SCC OnLine All 4254.
[50] Reserve Bank of India, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions,* RBI/2017-18/15 (July 6, 2017), https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336.*ns*.
[51] State Bank of India v. Pallabh Bhowmick & Ors., 2022 SCC OnLine Gau 1454.

two factors – instant reporting of the fraud and no evidence by the bank to prove negligence of the customer. The customer downloaded an app for returning the ordered garments on the direction of the fraudster posing as the customer care manager of the brand and subsequently, the amount was siphoned, later on the respondent company informed the customer that there was an illegal breach of the customer database whereby the information of their customers was leaked and the website was hacked when the online purchase was made.

Further, the Bombay High Court in the case of *Jaiprakash Kulkarni v. The Banking Ombudsman* held that the customer was the victim of third-party fraud and the bank was directed to bear complete liability.[52] In this case, the customer did not receive any OTP or SMS for the beneficiary that was added in their bank account the other day. The court found no evidence of negligence on the part of the customers and they proactively reported the matter to the cyber cell and banking ombudsman, in addition to raising a plea of blocking the SIM card to stop the transactions.

Thus, the interpretation of the Supreme Court and High Courts is varied and focuses on assessing the zero liability of the customer than on affixing liability on the PA or merchant bank in different cases. Moreover, clause 8 of the Directions focuses on creating a liability regime by way of contractual understanding, the clear liability will still depend on the different factors influencing the fraudulent transactions and is not certainly determined. Therefore, the Directions define roles and responsibilities but

[52] Jaiprakash Kulkarni v. The Banking Ombudsman, 2024 SCC OnLine BOM 1666.

the liability will differ contractually subject to different interpretations of the courts.

V. THE EUROPEAN FRAMEWORK ON FRAUD PREVENTION

The European Commission's PSD3, Payment introduced in June 2023, provides a comprehensive framework for strengthening fraud prevention in digital payments.[53] It builds on the existing Payment Services Directive 2 ("**PSD2**") and addresses emerging fraud risks, particularly impersonation fraud, also called "spoofing", and unauthorized credit transfers.[54]

One of the key provisions under PSD3 is the introduction of IBAN/name matching verification for all credit transfers, including instant payments. This system ensures that before a payment is completed, the name on the account is checked against the IBAN provided by the payer. If a discrepancy is detected, the payer receives a notification and can decide whether to proceed. This measure aims to prevent fraudulent transactions where victims are deceived into transferring money to unauthorised accounts. Each Payment Service Provider ("**PSP**") will have a legal basis to share fraud-related information with each other, ensuring compliance with the General Data Protection Regulation ("**GDPR**").

---

[53] European Commission, *Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market* (PSD3) (2023) (COM(2023) 366 final).

[54] European Parliament Directive, *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives* 2002/65/EC, 2013/36/EU and 2013/36/EU and repealing Directive 2007/64/EC OJ L 337/1 (2015) (337/58).

PSD3 also establishes a clear liability framework for PSPs, as under this directive, the PSP of the payer is held fully liable for a fraudulent credit transfer if it fails to notify the payer of a detected mismatch between the unique identifier and the name of the payee. Additionally, PSPs are responsible for fraudulent transactions where consumers have been manipulated into authorizing payments by fraudsters impersonating PSP employees.[55] To further enhance fraud prevention, PSD3 introduces an obligation for electronic communications service providers to cooperate with PSPs. This collaboration is intended to help detect and prevent fraud more effectively, particularly in cases where communication channels are exploited to deceive consumers.

Another significant reform under PSD3 is the expansion of refund rights for consumers affected by fraud.[56] Refund will be granted in two key situations; first, when a PSP fails to detect an IBAN/name mismatch, resulting in a fraudulent payment; and second, when a consumer falls victim to spoofing fraud.[57] However, refunds will not be available in cases of gross negligence, such as when a consumer repeatedly falls for the same type of fraud.[58]

---

[55] *Id.*

[56] João Courinha, *The Regulatory Ripple Effect: Fraud Management in the Wake of PSD3, PSR and FIDA*, WORLDLINE (Feb. 10, 2023), https://worldline.com/en/home/main-navigation/resources/blogs/2023/the-regulatory-ripple-effect-fraud-management-in-the-wake-of-psd3-psr-and-fida#:~:text=In%20addition%20to%20enhanced%20information,and%20detection%20mechanisms%20from%20PIs.

[57] Obsah stránky, *Payment Services: Revised Rules to Improve Consumer Protection and Competition in Electronic Payments*, EUR. COMM'N (June 28, 2023), https://ec.europa.eu/commission/presscorner/detail/cs/qanda_23_3544.

[58] *Id.*

VI. SUGGESTIONS FOR STRENGTHENING FRAUD PREVENTION POLICIES OF INDIA IN DIGITAL PAYMENTS ECOSYSTEM

India's current fraud prevention policies focus heavily on merchant compliance and transaction tracking; however, it does not sufficiently address advanced fraud techniques like social engineering and spoofing. While the Indian policy addresses KYC requirements and prohibits the storage of sensitive data, more can be done to tackle the sophisticated fraud risks highlighted by the European Commission.

A. ENHANCING ACCOUNT VERIFICATION MECHANISMS

First, similar to Europe's IBAN/name matching proposal, a verification mechanism where the name of the account holder is checked against the IFSC code and account number before finalising any credit transfer can be introduced. This would help prevent cases where fraudsters direct victims to make payments to unauthorised accounts and the impact of social engineering frauds by adding a layer of verification.

Recently, the RBI directed banks and financial institutions to integrate the FRI developed by the Department of Telecommunications.[59] The FRI was launched under the Digital Intelligence Platform to address the prevalent situation of financial frauds. This tool aims to provide advanced intelligence to Banks, Financial Institutions and digital payment platforms. It classifies mobile numbers into three categories, medium, high and very high, this tool will enhance cyber protection and validation checks

[59] *Supra* note 7.

in case of mobile numbers flagged with this tool when digital payment is proposed to be made to such numbers. The classification is made on the basis of feedback received from various stakeholders, including reporting on various government portals. The tool aims to prioritise enforcing high customer protection mechanisms in case a mobile number has a high risk. PhonePe and Paytm have integrated FRI in real time to take preventive measures such as declining suspicious transactions, issuing alerts or warnings to customers, and delaying transactions flagged as high risk.

However, the advisory is limited to banks and UPI service providers. In the domain of PA, another promising initiative that is being explored is the creation of a "negative database."[60] This centralised repository would store records of fraudulent transactions across customers and merchants, enabling financial institutions and aggregators to detect recurring fraud attempts across different platforms. By sharing fraud-related data, payment service providers can strengthen their ability to identify and prevent repeat offences.

However, presently, the Directions prohibit the storage of customer card credentials within its database, even when not accessible to the merchant, except for limited purposes for transaction tracking.[61] While the initiative aligns with the requirement of employing a risk management system, without a clearly defined scope of which type of data can be stored,

---

[60] Sachin K., *Payment Aggregators to Create 'Negative' Database to Tackle Digital Fraud*, FINANCIAL EXPRESS, (Sept. 2, 2024, 12:10 AM), https://www.financialexpress.com/business/banking-finance-payment-aggregators-plan-negative-database-to-combat-frauds-3598331/.

[61] RBI Master Direction on Regulation of Payment Aggregators, *supra* note 8, Annexure 2, recommendation 2.

it risks conflicting with existing regulations. Additionally, the initiative proposes sharing data on fraudulent transactions among PAs. Therefore, it is crucial to refine the proposal to align with regulatory frameworks while maximising its effectiveness in fraud prevention.[62]

B. ASSIGNING LIABILITY AND STRENGTHENING PAYMENT AGGREGATOR ACCOUNTABILITY

Second, as noted above in the policies of leading PAs, the burden of fraud prevention is primarily shifted on to merchants, leaving gaps in accountability across the payment ecosystem. To address this, policies should be aligned with the Directions that clearly define the role of PAs in fraud detection and prevention. Stricter compliance with the requirements, along with enhanced monitoring systems, can ensure that current fraud mitigation efforts are adequately implemented to achieve the purpose. Additionally, liability for fraud-related losses should be appropriately assigned to the party responsible for the system failure, whether it be the PA, the bank, or another intermediary.

C. EXPANDING CONSUMER PROTECTION AGAINST SOCIAL ENGINEERING FRAUDS

Finally, to further strengthen fraud prevention, consumer refund rights should be introduced in cases of spoofing or impersonation fraud. Currently, the *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions* framework limits the liability of

---

[62] *Id.*

customers in cases of contributory negligence of the bank and third-party breach notified by the customer.[63] As outlined in Paragraph 7(ii) and Table 2, customer liability is reduced effectively based on the time taken to report the fraud, where the responsibility for the unauthorised electronic banking transaction lies elsewhere in the system.[64] If the fraud is reported within three working days, the customer has zero liability. If reported between four to seven working days, liability is limited to either the transaction value or a predefined limit set by the bank. Beyond seven working days, liability is determined according to the bank's board-approved policy.

However, this framework excludes social engineering frauds where the customer has shared the payment credentials thereby authorising transactions under false pretenses. Since these transactions appear "authorised" from the customer's end, they often fall outside the scope of protections available for unauthorised transactions. The current approach fails to account for cases where the customer is deceived through sophisticated fraud. This narrows the protection available to the customer by limiting protection on cases of contributory negligence and third-party system failure and leaving the customer remediless in other cases.[65]

VII. CONCLUSION

This article examines the regulatory framework governing PAs and PGs in India, revealing significant structural gaps in the RBI (Regulation of

---

[63] Reserve Bank of India, *Customer Protection – Limited Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, (July 6, 2017), https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=2336.
[64] *Id*, para 7 table 2.
[65] *Id.*

Payment Aggregators) Directions, 2025. Despite recent regulatory updates, several critical vulnerabilities persist that undermine the effectiveness of India's digital payment fraud prevention ecosystem. The analysis demonstrates that the current Indian framework relies excessively on merchant KYC procedures and onboarding protocols while inadequately addressing sophisticated fraud mechanisms such as spoofing and social engineering attacks. This overemphasis on preliminary verification fails to establish ongoing fraud detection and prevention obligations for PAs throughout the transaction lifecycle.

Examination of the practices of Razorpay further reveals a concerning pattern wherein PAs systematically deflect liability for fraud-related losses onto merchants and financial institutions. This diffusion of responsibility creates accountability gaps throughout the payment chain, leaving consumers vulnerable and without clear recourse when fraud occurs. Moreover, the non-mandatory nature of critical baseline technological requirements for fraud monitoring systems in PGs further weakens the regulatory framework's protective capacity.

To address these deficiencies, the article analyses the European Union's PSD3, which offers a more holistic approach to fraud prevention. It mandates IBAN/name matching for credit transfers, ensuring that consumers are alerted to mismatches before a payment is completed. It establishes clear liability standards by holding the payer's Payment Service Provider responsible in cases of failure to notify discrepancies or impersonation-related fraud. The directive also imposes a duty on

electronic communications providers to coordinate with PSPs in fraud detection and prevention, and significantly enhances consumer refund rights in instances of IBAN mismatches or spoofing, subject only to exclusions for gross negligence.

Based on this comparative analysis, the article proposes three fundamental recommendations to strengthen India's digital payment ecosystem.

First, India should implement an account verification system similar to Europe's IBAN/name matching that cross-references account holder names with IFSC codes and account numbers before executing transfers. This verification layer would significantly mitigate the risk of misdirected payments resulting from social engineering attacks. This approach could be complemented by the proposed "negative database" initiative for sharing fraud intelligence across platforms, provided appropriate safeguards are established to ensure compliance with data protection regulations.

Second, the Directions must move beyond compliance-oriented liability regime and clearly delineate a framework that appropriately assigns accountability based on the actual point of system failure. This would prevent PAs from shifting responsibility to merchants and would incentivize robust security investments across all participants in the payment ecosystem.

Third, India must expand its consumer protection framework to encompass social engineering frauds that currently fall outside the scope of existing safeguards. The interpretation of the current Customer Protection

framework excludes seemingly "authorized" but fraudulently induced transactions such as social engineering frauds, leaving a significant protection gap that undermines consumer confidence in digital payment systems.

The integration of the above-mentioned recommendations will substantially strengthen India's payment security ecosystem. Ultimately, effective fraud prevention requires a coordinated approach that balances regulatory oversight with industry responsibility and the proposed recommendations can help build a more resilient digital payment infrastructure in India.

Nikhilesh Prajapati & Soumya Jain, *From Conflict to Coherence: Reforming India's Netting Insolvency Interface*, 12(1) NLUJ L. REV. 104 (2026)

FROM CONFLICT TO COHERENCE: REFORMING INDIA'S NETTING-INSOLVENCY INTERFACE

~ Nikhilesh Prajapati & Soumya Jain[*]

ABSTRACT

*The process of Close-out Netting ("**CoN**") is ubiquitous in modern financial markets, wherein, in the event of a default, derivative contracts are terminated and obligations surrounding them are accelerated to identify the final amount to be paid by one party. In India, this is governed by the Bilateral Netting of Qualified Financial Contracts Act, 2020 ("**Netting Act**"), wherein CoN arrangements have been given complete overriding precedence over the Insolvency and Bankruptcy Code, 2016 ("**IBC**"), raising significant concerns about undermining the rights of other creditors during an Insolvency. To address this, the article employs a comparative analysis of the interplay of CoN and Insolvency in the United Kingdom (**U.K.**) and the United States (**U.S.**), as these jurisdictions have developed financial markets and scholarly discourse on the interplay between CoN and Insolvency. Deriving prudent recommendations from these jurisdictions, the article suggests five targeted solutions – including fraud prevention, cross-border harmonisation, and standardised master agreements. These are operationalised through four concrete recommendations spanning legislative, regulatory, and institutional reforms. Structured to progress from conceptual*

[*] Nikhilesh Prajapati is a fifth year B.A., LL.B. (Hons.) student at Gujarat National Law University, Gandhinagar and Soumya Jain is a third year B.A., LL.B. (Hons.) student at Hidayatullah National Law University, Raipur.

grounding and issue identification to comparative analysis and prescriptive solutions, the article concludes that recalibrating the CoN-Insolvency interface is essential to balance financial market stability with the foundational principles of insolvency law in India.

TABLE OF CONTENTS

I. INTRODUCTION 108

II. CONCEPTUAL FRAMEWORK AND CORE CONFLICT 110

A. CLOSE-OUT NETTING 110

B. QUALIFIED FINANCIAL CONTRACTS (QFC) 112

C. INTERPLAY OF CON WITH INSOLVENCY 113

II. CORE ISSUE 114

A. NON-OBSTANTE CLAUSE OF IBC 114

B. NON-OBSTANTE CLAUSE OF THE NETTING ACT 115

III. COMPARATIVE ANALYSIS 117

A. U.K. APPROACH 119

B. U.S. APPROACH 124

IV. APPLICABILITY TO INDIA AND ECONOMIC IMPLICATIONS 127

A. INTERPLAY BETWEEN CON AND INSOLVENCY IN CROSS-BORDER TRANSACTIONS 127

B. PREVENTION OF CREATION OF NEW CON AGREEMENTS DURING INSOLVENCY 130

C. STANDARDISED CON AND MASTER CON AGREEMENTS 132

D. FRAUD PREVENTION 134

E. ENACTMENT OF MULTIPLE STATUTES TAILORED TO THE INTERPLAY OF CON AND INSOLVENCY 135

V. RECOMMENDATIONS 137

A. LEGISLATIVE AMENDMENT 137

B. REGULATORY REFORMS 138

C. CROSS-BORDER FRAMEWORK..... 139

D. INSTITUTIONAL REFORMS 140

VI. CONCLUSION..... 140

I. INTRODUCTION

Recently, the new CoN Regulations in Saudi Arabia have significantly reduced the impact of an insolvency moratorium on the operationalisation of CoN.[1] This has provided substantial relief to financial institutions in their quest to reduce liquidity crunches,[2] even though such changes can have various negative effects, including problems relating to the possible restructuring of a debtor during the insolvency period.[3]

This is in continuation of the long-standing debate about the viability and the regulatory framework surrounding CoN during an insolvency proceeding.[4] Also, due to the highly interconnected nature of the current financial system, the said issue is not limited to a single jurisdiction but is a significant problem in financial market regulation at a global level.[5] For instance, the unhindered operationalisation of CoN in one jurisdiction may bankrupt another entity of the same or different jurisdiction, which may have repercussions throughout the global financial system.[6]

From an Indian perspective, this problem is further magnified by the Netting Act, which governs the CoN regime of India, allowing for complete

---

[1] Close-out Netting and Related Financial Collateral Arrangements Regulation, 2025.

[2] LATHAM & WATKINS, https://www.lw.com/en/insights/close-out-netting-in-the-kingdom-of-saudi-arabia.

[3] Simon Gleeson & Thomas Werlen, *Close-out Netting, Insolvency and Resolution of Financial Institutions* (SSRN, Working Paper No. 2694285, August 2016).

[4] Vincent Johnson, *International Financial Law: The Case Against Close-out Netting*, 33 B.U. INT'L L.J 395, 395-397 (2015).

[5] INTERNATIONAL SWAP AND DERIVATIVES ASSOCIATION, https://www.isda.org/a/LPDDE/netting-isdaresearchnotes-1-2010.pdf.

[6] Klaus Lober, *Close-out Netting: Impact on Risk Management and Systematic Risk*, UNCITRAL (December 16-17, 2013), https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/b2_financial_contracts_2_loeber.pdf.

overriding effects over insolvency.[7] Hence, it leaves the majority of the Indian CoN regime in an inefficient position regarding its implementation during insolvency.

Moreover, to this date, the Netting Act has seen no judicial verdict regarding its interplay with insolvency.[8] Therefore, an analytical enquiry into the issues becomes quintessential. This article tries to address the same by suggesting changes to the Netting Act and the IBC.

To adequately conduct an analytical enquiry, the conceptual framework relating to CoN and its core conflict of complete overriding over insolvency is explained in Part II. Subsequently, the Non-Obstante Clauses of both the Netting Act and IBC are evaluated, to frame the core issue of the article in Part III. Further the article identifies concerns like currency fluctuations in cross-border transactions, creation of new CoN agreements post-insolvency, lack of uniformity in CoN agreements leading to regulatory grey areas and fraud prevention during CoN.

Hence, to suggest prudent changes for the alleviation of these concerns, Part IV analyses the interplay of CoN and Insolvency ("**interplay**") in the U.K. and U.S. to derive meaningful suggestions as developing jurisdictions including India adopts structural elements from U.K. and U.S. models to ensure legal certainty in netting arrangements

---

[7] Bilateral Netting of Qualified Financial Contracts Act, 2020, § 10, No. 30, Acts of Parliament, 2020 (India).

[8] TRILEGAL, https://trilegal.com/wp-content/uploads/2021/11/Bilateral-Netting-of-Qualified-Financial-Contracts-Act-2020.pdf.

while preserving insolvency objectives.[9] Further, these jurisdictions' well-documented case law, regulatory guidance and institutional oversight mechanisms provide comprehensive precedents directly applicable to India's nascent Netting-Insolvency framework.[10] Subsequently, the applicability of those suggestions in India, along with their economic implications, is delineated in Part V. Moreover, in Part VI, the article recommends practical changes in India for a robust CoN regime.

II. CONCEPTUAL FRAMEWORK AND CORE CONFLICT

To provide a succinct conceptual understanding of the article, the authors in this part of the article delineate the basic terminologies associated with the interplay between CoN and Insolvency. These terminologies include: (1) CoN, (2) Qualified Financial Contracts ("**QFC**"), (3) Insolvency and its interplay with CoN.

A. CLOSE-OUT NETTING

CoN is an advanced method of clearing financial liabilities in QFC markets.[11] It allows early termination of contractual obligations from either counterparty to a QFC transaction on the occurrence of a default as per the pre-existing CoN Agreement between the parties.[12] Subsequently, there is an acceleration of mutual obligations as per the current market standards,

---

[9] Robert R. Bliss & George G. Kaufman, *Close-Out Netting and Systemic Risk*, 30, J. FIN. SERV. RES. 2, 55-70 (2006).

[10] MATTHIAS HAENTJENS, FINANCIAL COLLATERAL, Ch. 8, *Close-Out Netting and Safe Harbours* (OXFORD LAW PRO, 2020).

[11] David Mengle, *Close-out Netting and Risk Management in Over-the-Counter Derevatives*, SSRN (June 10, 2010), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1619480.

[12] Paech, Philipp, *Close-Out Netting, Insolvency Law and Conflict of Laws* (LSE Legal Studies, Working Paper No. 14, 2014) ("**PAECH**").

hence leading to efficient calculation and settlement of the net balance.[13] In India, Section 2(e) of the Netting Act defines CoN as, *"a process involving termination of obligations under a qualified financial contract with a party in default and subsequent combining of positive and negative replacement values into a single net payable or receivable as set out in section 6."*[14]

To put it simply , CoN materialises when '*in the money contracts*' (where the party will likely be profitable) are set off against '*out of the money contracts*' (where the party will most likely not be profitable) in a transaction after which the remaining liabilities are calculated based on current market value, leading to the calculation of a final amount which one party owes to the other.[15]

The said practice is adopted because it (i) halts the ongoing fluctuations in the highly volatile QFC market and thus reduces relative exposure on ongoing derivative contracts and (ii) it prevents repetitive payments and hence reduces the total amount, by netting, and the offsetting obligations on those contracts.[16]

---

[13] Thomas Keijser, TRANSNATIONAL SECURITIES LAW, 55 (Oxford University Press, 2022).

[14] Bilateral Netting of Qualified Financial Contracts Act, 2020, § 2(e), No. 30, Acts of Parliament, 2020 (India).

[15] Edward R. Morrison & Joerg Riegel, *Close-out Netting and Insolvency* (Columbia Law and Economics, Working Paper No. 2425, 2009), https://scholarship.law.columbia.edu/faculty_scholarship/2425/.

[16] PAECH, *supra* note 13.

B. QUALIFIED FINANCIAL CONTRACTS (QFC)

In the modern financial markets, QFCs play an exemplary role in allowing the parties to trade in high-speed transactions with immense value and simultaneously allow CoN of their claims in case of default.[17] The first legislative definition of QFC was given in Section 210(c)(8)(D) of Title II of the Dodd-Frank Act,[18] wherein it provides an enumerative list of agreements that per se constitute QFCs and include Swaps, Repurchase, Securities, Commodity and Forward contracts (the umbrella term used for such contracts is 'Derivative Contracts').

In India, the definition of QFC adopted is inherently ambiguous. As per Section 2(n) of the Netting Act, a QFC means, *"a qualified financial contract notified by the authority under clause (a) of section 4."*[19] A QFC is, therefore, any financial contract that the designated authority officially notifies as such. It does not list specific contracts but instead refers to the designation power granted to the relevant authority under Section 4(a) of the Netting Act. Whereas, the statutory list under the Dodd-Frank Act grants immediate and unambiguous legal status to the most systematically significant and prevalent financial instruments, along with authority to the regulator to designate similar agreements as QFC, ensuring stability for market participants. Therefore, the absence of a precise and strict statutory definition of QFC fundamentally compromises the entire framework of

---

[17] Edward J. Janger, *Implementing Symmetric Treatment of Financial Contracts in Bankruptcy and Bank Resolution*, 10 BROOK. J. CORP. FIN. & COM. L. 155, 161-168 (2015).
[18] The Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010, § 205(4), 124 Stat. 1457 (U.S.).
[19] Bilateral Netting of Qualified Financial Contracts Act, 2020, § 2(n), No. 30, Acts of Parliament, 2020 (India).

CoN, which exclusively triggers on a QFC transaction. This regulatory vacuum creates a risk of fragmented application, potential over-regulation and misuse.

C. INTERPLAY OF CON WITH INSOLVENCY

On the other tangent of the core issue lies insolvency. The primary objective of the same is fair and equitable treatment to all the creditors, maximisation of creditor value and creation of a common pool of assets for the reconstruction of the debtor.[20] The insolvency regime of nearly every jurisdiction places more reliance on the revival of the debtor and postulates liquidation only in circumstances where revival becomes highly improbable.[21] Therefore, the law of insolvency mandates the protection of the debtor and creates conditions that ameliorate the prospects of its revival.[22]

On the contrary, the mechanism of CoN does not try to protect the insolvent party but tries to protect the counterparty. This is achieved by giving the CoN agreement an overriding effect over the moratorium, hence effectively allowing it to ignore the insolvency proceeding.[23] Additionally, CoN between two solvent parties becomes a matter of convenience, but

---

[20] *See generally*, V Finch, *The Measures of Insolvency Law*, 17, OXFORD J. LEGAL STUD. 227 (1997).
[21] Vijay Kumar Singh, *Modern Corporate Insolvency Regime in India: A Review*, NLS BLR 7, 23, 27-29 (2021), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1112&context=nlsblr .
[22] *Id.*
[23] ANDREW KEAY, GOVERNANCE WHERE THE COMPANY IS INSOLVENT BUT NOT IN AN INSOLVENCY REGIME, 105-172 (Elgaronline, 2022).

the same between a solvent and an insolvent party is more than a mere convenience, as the substantive rights of various other creditors are affected in the process.[24]

Since the overall objectives of CoN and Insolvency are in direct contradiction to each other, there is an inevitable clash between them. Hence, generally in various jurisdictions, the law walks a tightrope regarding the interplay between the law of Insolvency and CoN, which gives rise to legal ambiguities.

II. CORE ISSUE

In India, the legislative enactments for Insolvency and CoN are the Netting Act and the IBC, respectively. Both the Netting Act and IBC have a very wide Non-Obstante clause, i.e. providing precedence over other laws,[25] hence their interplay in the case of an insolvency becomes extremely important to understand. Moreover, to date, there has been no judicial interpretation of the said ambiguity, which is coupled with a lack of literature on the issue.[26] This further highlights the need for an analytical enquiry into the issue at hand.

A. NON-OBSTANTE CLAUSE OF IBC

The non-obstante clause under Section 238 of the IBC is reproduced below.

---

[24] ROBERT R. BLISS, *supra* note 10.
[25] Union of India v. G.M. Kokil, (1984) 2 SCC 196, ¶11.
[26] Umakanth Varottil, *Navigating Legal Conundrums: The Interplay Between India's Netting Act and the Insolvency Code*, INDIACORPLAW (June 22, 2025) https://indiacorplaw.in/2024/09/11/navigating-legal-conundrums-the-interplay-between-indias-netting-act-and-the-insolvency-code/.

> *"238- The provisions of this Code shall have effect, notwithstanding anything inconsistent therewith contained in any other law for the time being in force or any instrument having effect by virtue of any such law."*

A pertinent observation regarding Section 238 of the IBC is that it comes with a marginal note which states that "*Provisions of this Code to override other laws*", which again highlights the '*legislative intent*'[27] while enacting this statute.

The said clause gives IBC primacy over nearly every other legislation[28], which is done to give precedence to insolvency proceedings so that the distribution or reconstruction of the debtor's assets is done in an orderly fashion and a creditor race is prevented.[29]

B. NON-OBSTANTE CLAUSE OF THE NETTING ACT

Section 5(4) read with Section 10 of the Netting Act acts as a non-obstante clause of the said legislation and is reproduced below-

> *"5(4) Where a qualified financial market participant is subject to administration, then, notwithstanding,—*
>
> *(i) any stay, injunction, avoidance, moratorium or similar proceedings or any other order of a court, tribunal or authority, or*

---

[27] Uttam Das Chela Sunder Das v. Shiromani Gurdwara Parbandhak Committee, AIR 1996 SC 2133.
[28] Sara Jain, *Analysing the Overriding Effect of the Insolvency and Bankruptcy Code, 2016*, 13, NUJS. L. REV., 1 (2020).
[29] VIJAY KUMAR, *supra* note 22, at 23.

(ii) any order of adjudication or dissolution or winding up or resolution or insolvency, or

(iii) any rule, regulation, scheme, direction, guideline, circular or order,

made or issued under any law for the time being in force, close-out netting shall be applicable, and nothing contained therein shall affect the validity of close-out netting under this Act.

10-. Provisions of this Act to override other laws.—The provisions of this Act shall have effect, notwithstanding anything inconsistent therewith contained in any other law for the time being in force or any instrument having effect by virtue of any such law."

It is a general presumption that the legislature, while drafting legislation, has complete knowledge of all previous legislation.[30] Therefore, after a plain reading of the language of the above provisions, one may infer that the legislature intended to provide the Netting Act with complete overriding powers over IBC.

The authors argue against this plain and grammatical reading and contend that for the harmonious interplay between the Netting Act and IBC, substantial changes should be made to the provisions of both legislations.

The underlying logic behind the contention is that if the current framework continues unchanged, then the same would allow the prominent entities in the financial markets, usually the ones that are capable of dealing

[30] Union of India v. Venkateshan S, (2002) 5 SCC 285; Jaycee Housing (P) Ltd. v. High Court of Orissa, (2023) 1 SCC 549.

in QFC, to entirely skip the moratorium timeline of insolvency. This will allow them to receive pound for pound of their debt, which can have the effect of draining the financial resources of the smaller creditors, especially the operational creditors.

This can create a sense of distrust within the credit lending circles of the business ecosystem of India. Since the need for every kind of credit is ubiquitous and the absence of any form of credit would be detrimental to the overall state of economic growth,[31] the need to harmoniously construct CoN with IBC becomes important. Before delving into the reforms that can be included in the Indian framework, it is incumbent to analyse the frameworks existing in other jurisdictions on the concerned subject matter. In this regard, the next section discusses the framework for interplay between CoN and Insolvency in the U.K. and the U.S. and suggests potential learnings that can be taken from it.

III. COMPARATIVE ANALYSIS

The global adoption of CoN legislation, as underscored by International Swaps and Derivatives Association (**'ISDA'**), reflects its critical role in modern finance. For a meaningful examination of the interplay between CoN and Insolvency, jurisdictions with developed jurisprudence and robust scholarly discourse are more instructive.

[31] Binani Industries Limited v. Bank of Baroda & Anr, (2018) SCC OnLine NCLAT, ¶82.

Consequently, this Part conducts a comparative analysis of the U.K. and U.S. frameworks.

The regulatory approach regarding the interplay between CoN and Insolvency of each country is briefly mentioned in the following table, which serves as an analytical lens for subsequent discussion.

Aspect	**U.K.**	**U.S.**	**India**
Key Legislation/ Regulation	Financial Collateral Agreement Regulations, 2003.[32]	Bankruptcy Code (Title 11)[33], *Dodd-Frank Act.* [34]	Netting Act, 2020.[35]
Creation of new CoN Agreement during Insolvency	Not permitted.[36]	This issue has not been addressed.	Permitted.
Cross Border Framework	CoN is enforced as per the terms of	CoN is enforced as per the terms of	No framework (Adoption of

[32] The Financial Collateral Arrangements (No.2) Regulations 2003, SI 2003/3226 (U.K.) ("**FCAR**").
[33] CODE TITLE 11, 1978 (U.S.).
[34] Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010 (U.S.).
[35] Bilateral Netting of Qualified Financial Contracts Act, 2020, No. 30, Acts of Parliament, 2020 (India).
[36] FCAR, Reg. 12(2) (U.K.)

	the Agreement.[37]	the Agreement.[38]	Universalist Cross Border Insolvency approach also required).[39]
Single Regulatory Authority	Bank of England.[40]	Securities and Exchange Commission.[41]	Multiple Regulatory Authorities.[42]
Fraud Prevention	This issue has not been addressed.	CoN agreements made by fraud are explicitly impermissible.[43]	No framework

A. U.K. APPROACH

The principal legislation dealing with the substantive rights of the parties regarding CoN in the U.K. empowers the Bank of England to

[37] FCAR, Reg. 12(1) r/w Reg. 14.
[38] Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010, § 560 (U.S.).
[39] Soumya Jain and Sidh Baunthiyal, *Resolving India's Cross-Border Insolvency Concerns: A Comparative Jurisdictional Analysis,* XIV, NLIU L. REV. 135 (2025).
[40] FCAR, Reg. 12(5).
[41] PAECH, *supra* note 13.
[42] Bilateral Netting of Qualified Financial Contracts Act, 2020, § 2(c), No. 30, Acts of Parliament, 2020 (India).
[43] CODE TITLE 11, 1978, § 546 (U.S.).

oversee payment systems and safeguards netting arrangements against insolvency risks. The key regulation dealing with the procedural aspects of the same is the Financial Collateral Arrangements Regulations, 2003[44] ("**FCAR**").

The scope of the article is limited to the procedural aspect of CoN in the U.K.; therefore, the FCAR become of special importance to the article. The FCAR Regulations 10(1)(b)[45] and 12[46] to 14[47] deal with the specific issue of CoN during an insolvency, and hence, a detailed analysis of the same would prove fruitful.

Regulation 12(2)[48] of the FCAR stipulates that if either party has any actual or constructive knowledge about the insolvency proceedings against any other party, then a new CoN agreement cannot be created by either of them. The same is further cemented by Regulation 12(4),[49] wherein it is mandated that if the party had any knowledge of any current insolvency proceedings against them, then the Insolvency Rules 2016 would apply to them.

Ergo, the FCAR categorically mandates that in case the insolvency was known beforehand, a CoN agreement will not materialise. This prevents any creditor with a malevolent intent from decreasing the pool of the common assets of the debtor during the restructuring process by using

---

[44] FCAR.
[45] FCAR, Reg. 10(1)(b).
[46] FCAR, Reg. 12.
[47] FCAR, Reg. 14.
[48] FCAR, Reg. 12(2).
[49] FCAR, Reg. 12(4).

CoN, as they are not able to create a new agreement for CoN post initiation of insolvency. This strikes an astute balance between the rights of the parties to use CoN on their common debts and the right of the other creditors forming the common pool of assets during the insolvency proceeding.

Additionally, the said regulation proves to be even more helpful during restructuring. During the restructuring of the debtor, if one of the parties is allowed to create a new CoN agreement and subsequently fully enforce the same on their claim. It can result in draining of the already short funds of the debtor. Consequently, hampering the debtor's prospects of revival and resulted in significant value loss for the common pool of other creditors, whether financial or operational.

Furthermore, this provision in particular ensures that the prominent lending financial institutions are not able to exert increasing dominance over the insolvent business entity and skip the queue of asset devolution of the debtor as per the insolvency laws. Therefore, it ensures to strike a delicate balance between the rights of creditors among each other vis-à-vis the debtor in an insolvency proceeding, which is also a quintessential necessity of an insolvency proceeding.[50] The FCAR explicitly provides for the adoption of certain standard forms of CoN frameworks that need to be followed to draft a CoN agreement, like the ISDA Master

[50] WORLD BANK, *Principles for Effective Insolvency and Creditor and Debtor Regimes*, https://documents1.worldbank.org/curated/en/391341619072648570/pdf/Principles-for-Effective-Insolvency-and-Creditor-and-Debtor-Regimes.pdf.

Agreement or the 'FBF Master Agreement.'[51] Adoption of such a standard framework ensures standardised practices and leaves negligible room for deviation from the legislatively permitted ambit of a CoN Agreement.

In case of cross-border transactions, the FCAR excludes the applicability of the Insolvency (England and Wales) Rules 2016 (debts in foreign currency).[52] Moreover, FCAR mandates conversion into foreign currency or vice versa to be done as per the terms of the CoN agreement.[53] This is done to ensure that exposure is minimised in case of CoN of any derivative based on the value of any underlying asset, which can fluctuate based on currency conversion.[54]

Additionally, this minimises the credit exposure and possible drain which can happen due to the fluctuating rate of currency exchange in the global foreign exchange markets. This can prove to be especially beneficial for transactions done through derivatives based on forex exchange indexes.

The definition of CoN as given under Regulation 3(1)(a)[55] and 3(1)(b)[56] of the FCAR stipulates the twin conditions under which the same can only be triggered. Regulation 3(1)(a) allows CoN by way of accelerating the obligations of the parties so that the same are due immediately and then

---

[51] FRENCH BANKING FEDERATION, *FBF Master Agreement Relating to Transactions on Forward Instruments*, https://www.fbf.fr/en/fbf-master-agreement-relating-to-transactions-on-forward-financial-instruments/.
[52] Insolvency (England and Wales) Rules 2016, SI 2016/1024 (U.K.).
[53] FCAR, Reg. 14.
[54] Graham Yeowart & Robin Parsons, THE LAW OF FINANCIAL COLLATERAL, 435 (Edward Elgar Publishing, 2016).
[55] FCAR, Reg. 3(1)(a).
[56] FCAR, Reg. 3(1)(b).

determining the CoN amount with reference to the current market valuation, which is also called the '*condition novation approach*.'[57]

The second approach given by Regulation 3(1)(b), wherein after taking into account due from each party in respect to its obligations to the other party. Subsequently, the party that owes the larger sum is liable to pay the net sum to the other party. This is also called CoN by the '*set off approach*'.[58]

The aforesaid approaches bring CoN into the ambit of the regulatory framework in a manner which allows maximum possible autonomy to the parties to utilise CoN and simultaneously prevents arbitrary, irrational or male-fide usage of CoN. Moreover, after a closer look at the twin approaches mentioned above, it becomes clear that they mandate the termination of current contractual liabilities between the parties before any netting takes place, hence effectively minimising the scope of conflict between CoN and insolvency.

Lastly, in the '*conditional novation*' approach, the acceleration of the liabilities of either side ensures hypothetical completion of contractual liabilities and its calculation '*in futuro*'.[59] This can ensure that the insolvent debtor also receives fair compensation for their side of the obligations and liabilities.

---

[57] GRAHAM, *supra* note 57.
[58] *Id.*
[59] GRAHAM, *supra* note 57.

B. U.S. APPROACH

In the U.S., the law surrounding CoN eventuates from four different legislative enactments. The US Bankruptcy Code (Title 11), 1978,[60] which lays down the primary framework for bankruptcy proceedings in the U.S., also provides for Safe-Harbour Provisions[61] ("**SHP**"). The SHPs principally allow the unhindered operation of CoN even during automatic stay, which is known as a moratorium in India.

The Federal Deposit Insurance Act, 1950 ("**FDIA**")[62] and the Federal Deposit Insurance Corporation Improvement Act, 1991 ("**FDICIA**")[63] postulate a specialised resolution regime for financial institutions and also enhance the CoN autonomy available to the parties to such transactions. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010[64] prescribes different methods for the resolution/liquidation of a systemically important financial institution. These legislations collectively form the CoN regime in the U.S.

Unlike the Indian Regime, wherein the operation of CoN is governed only by the Netting Act, the U.S. legal regime has specialised statutes for specific situations resulting from the interplay of Netting and Insolvency, which is tailored to the specific needs of various conditions. Furthermore, unlike the Indian Netting Act, which is overly brief and undescriptive regarding the procedural functionalism of the operation of

---

60 CODE TITLE 11, 1978 (U.S.).
61 Paech, Philipp, *The Value of Insolvency Safe Harbours*, Final version in the Oxford Journal of Legal Studies, Forthcoming (LSE Legal Studies Working Paper No. 9, 2015).
62 Federal Deposit Insurance Act, 1950 (U.S.).
63 Federal Deposit Insurance Corporation Improvement Act, 1991(U.S.).
64 Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010 (U.S.).

close-out netting, the U.S. law displays an adequate balance wherein CoN is regulated to the extent that it does not hamper party autonomy.

The immunity provided to CoN agreements in the U.S. is highly magnified, as is evident by Section 560 of FDICIA,[65] which explicitly protects netting rights for nearly all derivatives transactions. In practice, the safe harbour regime permits financial institutions to exercise CoN rights regardless of the maturity status of the underlying obligations, provided that the contractual mechanism for termination and netting is properly set forth. This aligns with the overall objective of close-out netting since the same is intended to mitigate systemic risk in markets where gross exposures can be astronomical.

Furthermore, vide 11 U.S.C. Section 546(e)[66] and Section 546(g),[67] any CoN transaction is treated as final and exempted from the operation of other laws, including insolvency, unless that transaction is caused by intentional or actual fraud. This is a crucial innovation in the U.S. CoN law since it places a minimum caveat on the operation of CoN by not allowing such a transaction to be materialised if it is tainted by fraud. This is to preserve the party autonomy, which is a paramount necessity for the operationalisation of any contractual arrangement.[68]

---

[65] Federal Deposit Insurance Corporation Improvement Act, 1991, §560 (U.S.).
[66] The Bankruptcy Code, 11 U.S.C. § 546(e), 1978 (U.S.).
[67] The Bankruptcy Code, 11 U.S.C. § 546(g), 1978 (U.S.).
[68] Richard Heckinger, Ivana Ruffini & Kirstin Wells, *Over-the-Counter (OTC) Derivatives* in *Understanding Derivatives: Markets and Infrastructure*, 27 FEDERAL RESERVE

This crucial change needs to be implemented in India since the same can create a much-needed protection from fraudulent agreements or undertakings during the high-value CoN transactions. This will help in improving the overall operationalisation of party autonomy during the process of CoN. Additionally, the U.S. legislature, vide the enactment of Section 362(b)(27)[69], has exempted Master Netting Agreements ("**MNA**") from the operation of an insolvency moratorium.

Moreover, Section 546(j)[70] prevents the transfer of any assets covered under the MNA by the resolution professional. Therefore, cross-product CoN through MNA has been given legislative sanctity through the enactment of the above provisions. This is similar to the approach adopted in the U.K., wherein it is mandatory for the parties to enter into a specific legislatively mandated CoN agreement. This ensures that there is a standard form of CoN Agreements which are followed, hence setting an industry standard which is not completely unregulated and not also being over-regulated.

Moreover, in the U.S., the primary regulatory authority dealing with CoN disputes is the Securities and Exchange Commission ("**SEC**"),[71] which also receives inputs regarding the same from the U.S. Commodity Futures Trading Commission ("**CFTC**").[72] The same allows the smooth

---

BANK OF CHICAGO, 29 (2014). https://www.chicagofed.org/publications/understanding-derivatives/index.

[69] The Bankruptcy Code, 11 U.S.C. § 362(b)(27), 1978 (U.S.).

[70] The Bankruptcy Code, 11 U.S.C. § 546(j), 1978 (U.S.).

[71] PAECH, *supra* note 13.

[72] INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION, https://www.isda.org/a/B4YgE/Cross-product-Netting-Under-the-US-Regulatory-Capital-Framework.pdf.

operation of CoN even during the multiplicity of legislations. Furthermore, the same ensures that the dispute regarding CoN will be resolved by a single adjudicatory authority and hence prevents a clash of jurisdiction.

IV. APPLICABILITY TO INDIA AND ECONOMIC IMPLICATIONS

This part of the article establishes the applicability of the significant learning from the two jurisdictions in India, along with their economic implications, so that a complete picture regarding the said changes can be portrayed.

A. INTERPLAY BETWEEN CON AND INSOLVENCY IN CROSS-BORDER TRANSACTIONS

Currently, India does not have a robust cross-border insolvency regime[73] ("**CBI**"), which can result in significant challenges in efficient enforcement of CoN, if a default takes place across jurisdictions and a moratorium is declared in the foreign jurisdiction and vice versa.

The absence of recognition of foreign insolvency proceedings and the territorial nature of the Indian CBI framework[74] can pose a significant risk to the liquidity ratio of both the creditor and the debtor. This can create a credit crunch, wherein the India-based creditors can face insolvency because they are unable to recover their credit from the foreign insolvent

---

[73] SOUMYA JAIN, *supra* note 41.
[74] Andrea Perrone, *The Legal Enforcement of Close-Out Netting and Set-Off in Italy: A Comparative Perspective*, 19, NLSIR., 1 (2014).

entity due to the absence of a robust CBI framework. Moreover, the foreign-based creditor will also be uncertain regarding the validity of CoN enforcement in case of a cross-border default, hence diminishing their intent to invest in the country.

Therefore, in cross-jurisdiction transactions, adopting the "*conditional novation approach"*[75] to CoN, whereby obligations terminate immediately upon default as specified in the CoN agreement, with claims valued at current market rates, allows parties to enforce netting without awaiting foreign insolvency proceedings. This method mitigates liquidity risks by calculating net liabilities in the currency and timeframe stipulated in the CoN agreement, preventing post-default valuation fluctuations. Subsequently, calculating the claims of both parties in the same currency and time period as mentioned in the CoN agreement can facilitate preventing any further fluctuations in the total quantum of the liability.

Furthermore, the territorial and domestic nature of the Indian CBI regime can hamper the recognition of the overriding effect of a foreign CoN agreement on the insolvency of the debtor. Therefore, by adopting a universalist approach to CBI, the Indian Insolvency and CoN regime can interact better with the CoN enforcement during insolvency in a different jurisdiction and reduce avenues of dispute and litigation. The said change can improve creditor trust and increase the prospects of inflow of Derivative investments in the Indian Financial Markets. To materialise the

---

[75] Sarah Worthington, *Novation and Advance Consent*, 83, CAMB. L.J., 1 (2024), https://www.cambridge.org/core/journals/cambridge-law-journal/article/novation-and-advance-consent/423BE9B0EB7A4EFF54DE7C97082921A0.

same, India needs to model its CBI regime as per the UNCITRAL Model Law[76] on CBI.

Generally, when the entirety of a national financial market or its biggest players collapse, it sends shockwaves throughout the global markets. This can have the effect of depreciating the asset from which derivatives derive their value, hence creating further financial distress.[77]

The U.K. '*conditional novation approach',*[78] if utilised, can help in averting the conversion of the collapse of a single financial market into a global financial distress and minimising systemic risk.[79] The same will prevent the further deterioration of assets from which derivatives derive value and allow for currency conversion as per the CoN Agreement, therefore improving efficiency. Furthermore, it can help in preventing a '*chain reaction of insolvencies*'[80] by allowing parties to retain sufficient liquidity to continue with their business operations.

---

[76] UNICTRAL Model Law on Cross-Border Insolvency, https://digitallibrary.un.org/record/1487896/files/1997-model-law-insol-2013-guide-enactment-e.pdf.

[77] Stephen Valdez & Philip Molyneux, AN INTRODUCTION TO GLOBAL FINANCIAL MARKETS, 132 (Palgrave Macmillan, 2015).

[78] WORTHINGTON, *supra* note 78.

[79] Böger v. Jones Cotton Co., 103 Ala. 234 (Supreme Court of Alabama 1937).

[80] Howard Davies & David Green, GLOBAL FINANCIAL REGULATION: THE ESSENTIAL GUIDE, 8 (Polity Press, 2008).

B. PREVENTION OF CREATION OF NEW CON AGREEMENTS DURING INSOLVENCY

The FCAR prevents the mechanical creation of a new CoN Agreement in case either party had either actual or constructive knowledge about insolvency beforehand.[81] This makes it difficult for the debtor or the creditor to defeat the provision in case they want to enforce a new CoN agreement on the claim after initiation of insolvency. Further, this ensures that any creditor cannot enforce CoN in a way that unfairly jeopardises the rights of other creditors during insolvency.

Given that QFC or derivative contracts are usually large in value and traded by giant financial players of the market,[82] if the above-mentioned changes are in India, the prominent financial institutions would not be able to create a fresh CoN agreement post-insolvency initiation by exerting their financial dominance. Hence, it can act as a shield against the malevolent intent of the larger creditors to enforce CoN on the claim from the debtor subsequent to the initiation of insolvency, by disallowing the creation of a new CoN agreement post-insolvency. This would ensure that the overall pool of assets of the debtor is not unfairly reduced by a few creditors.

A domino effect of the aforementioned changes can be on the rights of the operational creditors ("**OCs**") in the Corporate Insolvency Resolution Process ("**CIRP**"). If creation and enforcement of a new CoN Agreement is unequivocally allowed during the restructuring process, then the plight of OC's would be further enlarged since the OC's are not allowed

---

[81] The Financial Collateral Arrangements Regulations 2003, Reg. 12(2) (U.K.).
[82] ROBERT R. BLISS, *supra* note 10.

to be a part of the Committee of Creditors[83] and are usually paid in negligible amounts in terms of liquidation or resolution.[84] Hence, inculcating the U.K. approach can also help in cementing the rights of the Operational Creditors by maximising the available pool of assets of the debtor and minimising the losses incurred by them due to insolvency.

It is vehemently argued by scholars such as Robert R. Bliss & George G. Kaufman in their work *Derivatives and Systematic Risk: Netting, Collateral and Closeout*[85] and Vincent R. Joshson in his work *International Financial Law: The Case Against Close-out Netting,*[86] that CoN allows the Financial Creditor to run after settling his claim in full, even after the insolvency is declared and does nothing to contain the risks created by large-scale financial institutions but merely allows them to transfer the same to third parties under the guise of risk-mitigation,[87] this can lead to fire sale of derivatives.[88] Such a fire sale can have serious implications, as derivatives would then be sold for much less than what they are worth, therefore devaluing their underlying assets also. Furthermore, this harms the reorganising prospects of the debtor, which is also in contradiction with the

---

[83] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 21 (India); Essar Steel India Ltd. Committee of Creditors v. Satish Kumar Gupta, (2020) 8 SCC 531.
[84] *Id.*
[85] Robert R. Bliss & George G. Kaufman, *Derivatives and Systematic Risk: Netting, Collateral and Closeout*, 2, JOURNAL OF FINANCIAL STABILITY, 55-77 (2006).
[86] VINCENT, *supra* note 4.
[87] Joanna Benjamin, FINANCIAL LAW, 1 (Oxford University Press, 2007).
[88] Andrew Verstein, The Failure of Contracts: Contract Law Scholarship and the Financial Crisis, 8, Brook. J. Corp. Fin. & Com. L., 1 (2013), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1201&context=bjcfcl.
.

primary purposes of insolvency, i.e. timely resolution and equal treatment of creditors.[89]

Moreover, by CoN, the risk takers are allowed to externalise the cost of their activities on innocent third parties, which in this case are the other creditors who form the common pool of the debtor's assets.[90]

Therefore, the prevention of the creation of a new CoN Agreement post initiation of insolvency would ensure that the pre-insolvency substantive rights of other creditors are not unduly marginalised in favour of a newly created agreement post insolvency. Moreover, it can also help in the stabilisation of derivative values created by the fire sale of derivatives by curbing the right to transfer risk in the guise of *'risk mitigation'*.[91]

C. STANDARDISED CON AND MASTER CON AGREEMENTS

As per Regulation 3(1), the statutory right of Netting in the U.K. is explicitly required to be in the form of a contract. On the contrary, in the Indian Netting Act under Section 3, which deals with the applicability of CoN, the words enshrined are "*under a netting agreement or otherwise*". The usage of the word "*otherwise*" can extend the applicability of the act more than what should be legislatively or prudently permitted.

Hence, adopting a stricter and more exhaustive language regarding the applicability of CoN, as done in the U.K., can prove to be more fruitful, because the same would prevent the funnelling of various agreements in the garb of CoN agreements. Moreover, as per Section 2(j) of the Netting

---

[89] *Id.*
[90] VINCENT, *supra* note 4.
[91] JOANNA, *supra* note 90.

Act, the term netting is defined, but it is also mentioned that netting would include CoN. This can create ambiguity as a specialised definition of CoN is given under Section 2(e) of the Netting Act. Therefore, adopting a watertight approach regarding the definition of CoN, like in the U.K. law, can help in reducing the conflict between Netting and CoN.

Furthermore, in some cases, due to the acceleration clause of CoN, the counterparty to the agreement may face bankruptcy due to its inability to absorb the shock of the accelerated obligations.[92] Therefore, taking a liberal approach like using the word "otherwise" in the applicability clause of the Netting Act should be discouraged, as it may allow various '*macro-prudentially risky agreements*'[93] to be funnelled under the garb of CoN agreements.

Moreover, providing a draft Netting structure similar to the Master Netting Agreement, as done in the USA, based on the lines of the ISDA master netting agreement, can help in increasing the efficiency of Cross-product Netting. Moreover, such a framework can align the Indian CoN framework with international standards, hence increasing the ease of cross-product CoN both within and outside the country. Subsequently, this will also help in ensuring that the CoN framework is regulated in a manner that

---

[92] Sylvie A. Durham, DERIVATIVES DESKBOOK: CLOSE-OUT NETTING, RISK MITIGATION, LITIGATION, 1 (Practising law Institute, 2025).

[93] Rizwaan Jameel Mokal, *Liquidity, Systemic Risk, and the Bankruptcy Treatment of Financial Contracts*, BROOK. J. CORP. FIN. & COM. L. (2015) https://brooklynworks.brooklaw.edu/bjcfcl/vol10/iss1/2/.

neither harms the party autonomy nor allows it to be completely unregulated.

According to economic estimates, CoN, if executed properly, helps in reducing the overall exposure by eighty-five per cent.[94] Moreover, it also allows the regulated financial institutions to set aside regulatory capital for the net exposures rather than the gross exposures represented by the individual transactions.[95] Therefore, the adoption of standard CoN Agreements is necessary to harness the above advantages of CoN with minimum delays and create an apt regulatory framework for the same.

Additionally, providing a blanket protection to CoN Agreements may also lead to diminished market discipline by reducing the incentive of the parties to a SFT or a Derivative Agreement to monitor the actions of their counterparty unless there is a general increase in the monitoring by other general creditors of these counterparties.[96]

C. FRAUD PREVENTION

Under the current Indian CoN regime, there is no bar on the enforcement of CoN even if the same is made or being enforced by either party using fraud. Moreover, Section 66 of the IBC, which allows the NCLT to set aside fraudulent transactions, will also not be functional in such a situation, as the Non-Obstante clause of the Netting Act, 2020, would

---

[94] INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION, https://www.isda.org/a/USiDE/netting-isdaresearchnotes-1-2010.pdf.

[95] INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION, https://www.isda.org/a/mIxgE/Navigating-Bankruptcy-in-Digital-Asset-Markets-Netting-and-Collateral-Enforceability.pdf.

[96] Frank Partnoy & David A. Skeel, Jr., The Promise and Perils of Credit Derivatives, 75, U. Cin. L. Rev. 1019, 1049 (2007).

exclude its applicability. This can incentivise parties to utilise fraud, which can have negative consequences regarding the sanctity of party autonomy during the process of CoN.

To address this critical gap, India could draw lessons from the U.S. CoN regime. U.S. law explicitly prohibits the enforcement of CoN agreements obtained through fraud.[97] Introducing a similar fraud exception clause is strongly recommended for India. Such a provision would effectively regulate CoN by preserving genuine party autonomy and nullifying fraudulent transactions. Therefore, a specific amendment to the Netting Act is necessary to prevent parties from enforcing CoN transactions tainted by fraud.

D. ENACTMENT OF MULTIPLE STATUTES TAILORED TO THE INTERPLAY OF CON AND INSOLVENCY

The presence of multiple statutes tailored to the specific needs of dealing with intricate issues of the interplay of CoN with insolvency in the U.S. CoN regime is a predominant reason for its efficiency. Subsequently, to reduce clashes in jurisdiction regarding Disputes related to CoN, the U.S. regime has empowered the SEC to resolve disputes and act as the chief regulator of CoN.[98]

In contrast, the Indian Netting Act is highly descriptive regarding the interplay of CoN and Insolvency. Therefore, there is a specific need to

---

[97] BENJAMIN, *supra* note 89.
[98] Franklin Allen & Douglas Gale, *Systemic Risk and Regulation* (SSRN Working Paper No. 1323190, December 2004).

supplement the Netting Act with statutes or regulations that help in a robust interaction between CoN and Insolvency. Moreover, in India, the appointment of a single authority for the regulation and dispute resolution of CoN becomes necessary, because the same would highly reduce the clash of jurisdiction. Furthermore, the dispute subject matter related to CoN may be highly mathematical and technical; hence, it would be prudent to empower a single tribunal (which possesses the requisite technical skills) to deal with such disputes.

Before the enactment of the Dodd-Frank Act, Safe Harbour clauses in the U.S. provided an incentive to regulatory arbitrage by encouraging parties to design products and strategies that shift the assets from the banking book to the trading book. This increased the systemic risk factor in the market.[99] Moreover, Safe-Harbour clauses created a kind of artificial channel for these transactions, which thereby operated with negligent regulatory oversight. This created social subsidisation of such transactions, hence leading to the detriment of normal financial contracts in favour of special financial contracts.[100]

This aptly displays how the unbridled usage of CoN can result in a loss for the public at large by allowing a few financial contracts to subsidise private losses by using CoN. Subsequently, to rectify the same, the Dodd-Frank Act[101] was enacted, and the interplay between CoN and insolvency

---

[99] William J. Bergman, Robert R. Bliss, Christian A. Johnson & George G. Kaufman, *Netting, Financial Contracts, and Banks: The Economic Implications* (SSRN Working Paper No. 505965, January 2004).

[100] *Id.*

[101] Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010 (U.S.).

was worked out in a manner that prevented the subsidisation of private losses by CoN. This improved the overall economic efficiency of the financial markets by preserving the capital of the depositors to the best possible extent.[102]

The current Indian position on CoN is similar to the U.S. before its enactment of the Dodd Frank Act; therefore, the Indian regime is also running on the risk of social subsidisation of private losses. Hence, to reduce social subsidisation, specific legislation and regulations which provide for harmonious interplay between Netting and CoN are needed to supplement the currently undescriptive and highly pro-creditor Netting Act.

V. RECOMMENDATIONS

A. LEGISLATIVE AMENDMENT

A coherent statutory framework is indispensable to reconcile the functional objectives of close-out netting with the foundational principles of insolvency law. As demonstrated in this article, both the Netting Act and the IBC warrant substantive legislative reform. *First*, Section 3 of the Netting Act should be amended to delete the phrase "*or otherwise*," thereby limiting the statute's applicability strictly to contractually valid netting arrangements and preventing the funnelling of agreements in the garb of

---

[102] Akber Datoo, Paul Williams & Rhodri Whiteley, *A New Approach to Close-Out Netting Legal Opinions in Respect of OTC Derivatives and Securities Financing Transactions*, 15, J. SEC. OPER. & CUSTODY, 260 (2023).

CoN. *Second*, the Act must incorporate an exhaustive, contract-specific definition of close-out netting modelled on the UK's FCAR to eliminate ambiguity and prevent overlap with general netting mechanisms. *Finally*, the current conflict arising from the overlapping non-obstante clauses in the two statutes necessitates careful recalibration to ensure a balanced approach regarding the operationalisation of netting agreements so that the same does not unconditionally override critical insolvency safeguards.

B. REGULATORY REFORMS

Strengthening of regulatory underdevelopment is required for the effective operation of netting to ensure a balance between preserving market efficiency and upholding the equitable distribution objectives inherent in insolvency law. To this end, the regulatory framework should mandate the use of recognised master netting agreements, such as the ISDA or FBF Master Agreements for QFCs, as is the practice under the U.K.'s FCAR to enhance uniformity, legal certainty, and enforceability. Complementing this, the development of draft templates or model frameworks for close-out netting agreements akin to the U.S. Master Netting Agreement structure would provide much-needed clarity and consistency in netting arrangements.

In addition to standardisation, the regulatory regime must incorporate substantive safeguards to ensure that close-out netting does not operate to the detriment of broader insolvency objectives. An express prohibition on creation or enforcement of new CoN agreements after initiation or reasonable anticipation of insolvency proceedings, as reflected in Regulation 12 of the U.K.'s FCAR, is encouraged for preventing

opportunistic behaviour by financially dominant creditors who may otherwise seek to extract value from the debtor's estate at the expense of other stakeholders. Further, the Netting Act must include a specific fraud exception clause, drawing from the U.S. Bankruptcy Code Section 546(g), to ensure that CoN agreements procured through fraudulent conduct are rendered void.

C. CROSS-BORDER FRAMEWORK

The absence of a coherent cross-border insolvency framework under the Indian regime poses significant challenges to the enforceability of close-out netting arrangements. An internationally aligned regime is essential to mitigate jurisdictional conflicts and enhance transactional certainty in cross-border financial contracts. The U.K.'s FCAR offers instructive guidance for India's territorially confined regime. The U.K.'s FCAR exempts foreign currency debts from the application of the domestic insolvency rules and instead mandates that currency conversions be executed strictly in accordance with the terms stipulated in the CoN agreement. India must replicate this clarity by mandating that all cross-border CoN agreements specify valuation currencies and timelines. Moreover, India should adopt the "*conditional novation*" approach, under which obligations under CoN agreements are terminated immediately upon default and valued at prevailing market rates, rather than being subjected to delays from foreign insolvency proceedings. To operationalise this, India must reorient its CBI regime in line with the UNCITRAL Model Law on

Cross-Border Insolvency, thereby transitioning from a territorial to a universalist framework.

D. INSTITUTIONAL REFORMS

Institutional coherence will further enhance legal certainty and ensure the effective implementation and adjudication of close-out netting within the insolvency framework. The current Indian framework has a fragmented oversight by different regulatory authorities. Drawing from the U.S. experience, where agencies like the SEC and CFTC exercise consolidated jurisdiction over netting and derivative markets, India must consider appointing the RBI as a single regulatory authority to govern all aspects of CoN enforcement. In parallel, a specialised adjudicatory authority within the RBI itself, equipped with the necessary financial and technical expertise, should be established to handle netting-related disputes, particularly those involving complex valuations or derivative calculations. Furthermore, the Indian regime should consider developing an institutional oversight mechanism akin to the Dodd-Frank framework to monitor systemic CoN practices and prevent regulatory circumvention.

VI. CONCLUSION

The unresolved overlapping of non-obstante clauses of the Netting Act and IBC epitomises a regulatory schism that jeopardises both creditor equity and market stability. With no judicial resolution, this fundamental tension between the two legislations creates a '*tug of war*' and exacerbates legal uncertainty. As demonstrated in this article, the status quo enables regulatory arbitrage by dominant financial actors and drains assets meant

for the revival of operational creditors and debtors through CoN enforcement, an outcome irreconcilable with global frameworks.

In *summum bonum,* the article tried to positively contribute towards unravelling this vexatious interplay of CoN and Insolvency by delineating the current applicable law regarding the interplay in the UK and US and identifying potential solutions for India from these jurisdictions, along with economic implications. As a direct outcome of this comprehensive study, the authors unequivocally conclude that India's current CoN regime, characterised by its inefficiencies and complete overriding powers over insolvency, is neither legally sound nor economically appropriate. Reconciling these regimes is not merely doctrinal but essential for India's financial ecosystem. Adopting reforms from these jurisdictions would position India's Co alongside global jurisdictions like the UK and US, where CoN reduces exposure by 85% without compromising insolvency revival goals.

This synergy will bolster cross-border transactions, prevent chain-reaction insolvencies, and align with the IBC's original vision of preserving value through equitable restructuring. Unamended, the Netting Act risks becoming a legislative relic that fuels creditor races rather than curbing them. By embracing calibrated reforms, India can transform this '*tug of war*' into a harmonised framework that balances market efficiency with the IBC's revival ethos.

NLUJ Law Review

Harsh Manglam, *Regulating Tokenised Assets: A Comparative Analysis of Legal Frameworks, Banking Integration, and Future Policy Directions*, 12(1) NLUJ L. REV. 142 (2026)

REGULATING TOKENISED ASSETS: A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS, BANKING INTEGRATION, AND FUTURE POLICY DIRECTIONS

~ Harsh Manglam[*]

ABSTRACT

The rise of tokenised assets has introduced new complexities in banking, finance, and digital ownership, necessitating a robust legal and regulatory framework. However, the lack of uniform classification and regulatory clarity presents significant challenges for financial institutions, investors, and policymakers. The primary problem explored in this research is the regulatory uncertainty surrounding tokenised assets, especially regarding their classification as securities, commodities, or property, compliance with banking laws, and enforcement mechanisms in cross-border transactions. The purpose of this research is to provide a comparative analysis of regulatory approaches in key jurisdictions, including the United States, the European Union, and India, while examining the role of central banks, financial institutions, and legal systems in governing tokenized assets. Through a detailed review of case studies, this study evaluates the real-world implications of regulatory decisions on the tokenised financial ecosystem. The findings of the research expose

[*] Harsh Manglam is a fifth-year student at School of Law, GITAM (Deemed to be University), Vishakapatnam, Andhra Pradesh.

regulatory fragmentation, compliance risks, and legal uncertainties that hinder the widespread adoption of tokenised assets. The research highlights the need for harmonised global regulations, legal clarity on smart contracts, and enhanced investor protections. The findings suggest that central banks and financial regulators must adopt a balanced approach that fosters innovation while maintaining financial stability. By addressing legal uncertainties, strengthening compliance measures, and promoting cross-border cooperation, tokenised assets can be securely integrated into mainstream banking and financial markets, unlocking their full economic potential.

TABLE OF CONTENTS

I. INTRODUCTION 147

A. RISE OF TOKENISED ASSETS IN BANKING AND FINANCE 148

B. RELEVANCE OF TOKENISATION TO DIGITAL OWNERSHIP AND BANKING LAW 150

II. TOKENISED ASSETS AND DIGITAL OWNERSHIP 153

A. ROLE OF BLOCKCHAIN IN TOKENISATION 153

B. LEGAL RECOGNITION OF DIGITAL OWNERSHIP: PROPERTY RIGHTS VS. SECURITIES LAWS 156

III. GLOBAL REGULATORY APPROACHES TO TOKENISED ASSETS 159

A. UNITED STATES: A FRAGMENTED YET ROBUST REGULATORY LANDSCAPE 159

B. EUROPEAN UNION: A UNIFIED YET STRINGENT FRAMEWORK 162

C. INDIA: A CAUTIOUS BUT EVOLVING REGULATORY APPROACH 164

IV. KEY CHALLENGES IN INTEGRATION OF BANKING AND TOKENISED ASSETS 167

A. REGULATORY UNCERTAINTY AND COMPLIANCE RISKS 167

B. CUSTODY AND SECURITY CONCERNS 168

I. CUSTODIAL V. NON-CUSTODIAL SERVICES 168

II. CYBERSECURITY AND FINANCIAL STABILITY ISSUES: ..168

C. BANK COMPLIANCE AND FRAUD PREVENTION..... 169

I. RISKS OF MONEY LAUNDERING AND FRAUDULENT TRANSACTIONS..... 169

II. BANK OBLIGATIONS 170

D. CONSUMER PROTECTION AND FINANCIAL INCLUSION 170

I. RETAIL INVESTOR RISKS AND MARKET MANIPULATION 171

II. ENSURING SECURE ACCESS FOR CONSUMERS THROUGH BANKS 171

V. REAL-LIFE CASE STUDIES ON TOKENISED ASSETS AND BANKING LAW 172

A. SEC VS. RIPPLE (XRP): THE SECURITIES CLASSIFICATION DEBATE 173

B. BNY MELLON'S CRYPTO CUSTODY SERVICES 175

C. THE DAO HACK: SMART CONTRACT VULNERABILITIES AND LEGAL ACCOUNTABILITY 177

VI. POLICY RECOMMENDATIONS FOR THE ADOPTION OF DECENTRALISED FINANCE 178

A. THE ROLE OF CENTRAL BANKS IN TOKENISED ASSET REGULATION 179
B. RECOMMENDATIONS FOR POLICYMAKERS AND FINANCIAL INSTITUTIONS 181
VII. CONCLUSION AND OBSERVATION 183

I. INTRODUCTION

Technology, across sectors, is drastically transforming the very foundation of industries; the financial sector is no exception. However, this transformation is not without potential risks. Regulators must develop new approaches to regulate the use of technology, balancing the benefits and risks. of financial stability and consumer protection. Tokenisation of assets,[1] be it digital or physical, is revolutionising the financial sector by digitising ownership rights and enabling seamless transactions on blockchain networks.[2] This transformation has significantly impacted various sectors, such as banking law, financial regulation, and digital ownership rights[3]. Tokenisation of assets ensures efficiency, transparency, and enhanced liquidity, their integration into the traditional financial and banking systems presents complex legal and regulatory challenges. Numerous innovative technologies have resulted in the development of financial technology, which promises innovation and economic growth by challenging traditional financial services businesses.

The paper seeks to first briefly discuss the concept of tokenization and digitization of banking industry, secondly conceptualise the relevance of blockchain technology with the future of banking, while analysing the core characteristics of digital assets, in a comparative ecosystem, further,

---

[1] BOSTON CONSULTING GROUP *et al.*, *IMPACT OF DISTRIBUTED LEDGER TECHNOLOGY IN GLOBAL CAPITAL MARKETS* 6 (2023).

[2] Misha Tsukerman, *The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 BERKELEY TECH. L.J. 1127, 1140 (2015).

[3] *Supra* note 1, at 2.

the study seeks to draw a comparison between the legal systems governing digital assets in the USA and the European Union, and the scattered system that currently exists in India, and further analysing the present and persistent challenges that the current digital assets ecosystem poses before the regulators. Furthermore, examining case studies to better understand the implementation of digital assets in the present finance ecosystem. Lastly, the study seeks to present possible amendments and changes that could be implemented in the present ecosystem to better utilize this technology. Overall, this paper seeks to contribute to the ongoing legal conundrum on tokenized assets, offering practical policy solutions for integrating tokenization into banking law while ensuring financial stability and legal certainty.

A. RISE OF TOKENISED ASSETS IN BANKING AND FINANCE

Tokenisation of assets refers to the process of converting ownership of physical assets into digital tokens that are stored, traded, and represented on a blockchain[4]. This increases the fungibility of assets, allowing them to be divided into smaller units and transferred digitally with greater efficiency and reduced costs.[5] Unlike traditional financial systems, tokenisation leverages smart contracts and decentralised ledger technology to facilitate peer-to-peer transactions with enhanced security, transparency,

---

[4] WORLD ECON. F., *DIGITAL ASSETS, DISTRIBUTED LEDGER TECHNOLOGY, AND THE FUTURE OF CAPITAL MARKETS* 6 (2023), https://www.weforum.org/reports/digital-assets-distributed-ledger-technology-and-the-future-of-capital-markets/.

[5] INT'L INST. FOR SUSTAINABLE DEV., *TOKENIZATION OF INFRASTRUCTURE: A BLOCKCHAIN-BASED SOLUTION TO FINANCING SUSTAINABLE INFRASTRUCTURE* IV (2019).

and automation.[6] Tokenisation minimises settlement times, lowers transaction costs, and increases liquidity by allowing fractional ownership, meaning that high-value assets such as commercial real estate or fine art can be divided into smaller, tradable digital tokens. The technology has the potential to democratise access to investment opportunities, allowing a broader range of retail and institutional investors to participate in sectors that were previously restricted to retail investors due to entry barriers.[7]

Asset tokenization has gained widespread traction with the rise of blockchain technology and decentralized finance, as there is an ever-increasing demand for an efficient and transparent financial regime.[8] Several key milestones have shaped the evolution of tokenized assets and their intersection with banking and financial systems. The emergence of Security Token Offerings,[9] which comply with securities laws unlike the earlier Initial Coin Offerings,[10] has allowed institutional investors to engage with tokenised assets in a regulated manner. Major financial institutions have

---

[6] Abdulgaffar Muhammad and Aisha Ahmad Ishaq, *Decentralized Finance ("**DeFi**") and Traditional Banking: A Convergence or Collision*, 5 ECON. POL. & REGIONAL DEV. 1, 5 (2024); *See also* BOSTON CONSULTING GROUP *et al. supra* note 1, at 2.

[7] *See*, Ashutosh Gupta, Jash Rathod, et al., *Tokenization of Real Estate Using Blockchain Technology*, in *APPLIED CRYPTOGRAPHY AND NETWORK SECURITY WORKSHOPS* (Proc. of Oct. 14, 2020), https://doi.org/10.1007/978-3-030-61638-0_5.

[8] Agustín Carstens and Nandan Nilekani, *Finternet: The Financial System for the Future* (Bank for Int'l Settlements, Monetary & Econ. Dep't Working Paper, 2024).

[9] DELOITTE *et al.*, *SECURITY TOKEN OFFERINGS: THE NEXT PHASE OF FINANCIAL MARKET EVOLUTION?* 6 (2018); *See also,* Thomas Lambert, Daniel Liebau, *et al.*, *Security Token Offerings*, 59 SMALL BUS. ECON. 303 (2021).

[10] *See*, Sabrina T. Howell, David Yermack Kerman, *et al.*, *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, 30 REV. FIN. STUD. 3925, 3926 (2020); *See also* Shaanan Cohney *et al.*, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591 (2019).

begun offering tokenised securities and digital asset custody services, demonstrating the growing institutional interest in this space. Governments and financial regulators across the globe have been actively formulating policies to address the numerous challenges arising from tokenisation, as observed in Markets in Crypto-Assets,[11] regulation in the European Union, and the U.S. Securities and Exchange Commission's evolving stance on digital securities. Furthermore, the rise of Central Bank Digital Currencies,[12]such as China's Digital Yuan,[13] the European Union's Digital Euro,[14] and India's Digital Rupee,[15] showcases the increasing role and demand for government-backed digital financial ecosystems in shaping the tokenisation landscape.

B. RELEVANCE OF TOKENISATION TO DIGITAL OWNERSHIP AND BANKING LAW

The rise of tokenisation of assets has fundamentally reformed the idea of ownership, banking operations, and financial regulations by shifting from centralised asset registries to decentralised blockchain-based digital records.[16] The conventional ownership of assets, be it digital or physical assets, is established through physical documentation, government-backed

---

[11] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets, 2023 O.J. (L 150) 40.

[12] Raphael Auer*et al.*, *Rise of the Central Bank Digital Currencies*, 19 INT'L J. CENT. BANKING 185 (2023); *See also* John Kiff *et al.*, *A Survey of Research on Retail Central Bank Digital Currency* (Int'l Monetary Fund Working Paper, 2020).

[13] *See* Martin Chorzempa, *China, the United States, and Central Bank Digital Currencies: How Important Is It to Be First?* 14 CHINA ECON. J. 104 (2021).

[14] EUR. CENT. BANK, *REPORT ON A DIGITAL EURO* 7 (2021).

[15]RESERVE BANK OF INDIA, *DIGITAL RUPEE*, https://www.rbi.org.in/commonman/English/scripts/FAQs.aspx?Id=3686.

[16] ORG. FOR ECON. CO-OPERATION & DEV., *REGULATORY APPROACHES TO THE TOKENISATION OF ASSETS* 15 (2021).

registries, and legally recognised intermediaries. However, tokenised assets exist in a purely digital form, where ownership is represented by cryptographic tokens stored on a blockchain ledger, often without a central authority overseeing transactions.[17]

This transformation raises numerous legal questions with regard to the recognition, enforcement, and transferability of digital ownership rights. Additionally, the lack of global standardisation in defining tokenised property rights creates legal uncertainty for investors and financial institutions, as different jurisdictions may classify the same asset in varying legal categories ranging from securities to commodities or intangible property.[18] These inconsistencies have complicated cross-border transactions and increased compliance burdens for businesses and investors engaged in the tokenised asset ecosystem.[19]

Tokenisation drastically challenges the traditional roles of banks as custodians and intermediaries in financial transactions. Since tokenisation is based on direct peer-to-peer transactions, it potentially reduces the reliance on banks for asset transfers and financial settlements. Despite these changes, banks remain critical players in the digital asset space due to their expertise in risk management, regulatory compliance, and asset security.

---

[17] Iota Kaousar Nassr, *Understanding the Tokenisation of Assets in Financial Markets* (OECD Publication 2021).

[18] AKASH GADIYA, *OVERVIEW OF DIGITAL ASSET* 25–26 (S. INDIA REG'L COUNCIL, INST. OF CHARTERED ACCOUNTANTS OF INDIA, 1ST ED. 2022).

[19] TOKENISED CMTY. COUNCIL, *DIGITAL ASSET CLASSIFICATION: NEEDS AND CHALLENGES IN A RAPIDLY EVOLVING ENVIRONMENT*, https://www.tokenizedcommodities.org/post/digital-asset-classification-needs-and-challenges-in-a-rapidly-evolving-environment.

Financial institutions are now exploring digital asset custody services to safeguard tokenised securities and cryptocurrencies, while also ensuring compliance with Anti-Money Laundering and Know Your Customer regulations.[20]

The integration of tokenised assets into regulated financial systems poses unique challenges, as regulators across the globe are debating issues such as whether banks should be allowed to hold tokenised assets, how digital asset custody should be structured, and who bears liability in the event of a cybersecurity breach or fraud. Further, taxation of digitally owned assets remains another ambiguous subject, whether these assets are subject to capital gains taxes or not, and how to trace taxable transactions in decentralised networks.[21]In the absence of a universally accepted legal framework, tokenised assets remain vulnerable to risks such as fraud, regulatory arbitrage, smart contract failures, and jurisdictional conflicts. Legal frameworks must ensure a balance between financial innovation and investor protection, thereby reducing systemic risks while promoting the adoption of digital assets in mainstream banking and financial markets.[22]

---

[20] ORG. FOR ECON. CO-OPERATION & DEV., *REGULATORY APPROACHES TO THE TOKENISATION OF ASSETS* 20 (2021).

[21] Katherine Baer, Ruud De Mooij, et.al., T*axing Cryptocurrencies*, 39OXFORD REV. ECON. POL'Y485 (2023); Misha Tsukerman, *The Block Is Hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future*, 30 BERKELEY TECH. L.J. 1127, 1147 (2015).

[22] BANK FOR INT'L SETTLEMENTS, *SOUND PRACTICES: IMPLICATIONS OF FINTECH DEVELOPMENTS FOR BANKS AND BANK SUPERVISORS* 29 (2018), https://www.bis.org/bcbs/publ/d431.pdf.

II. TOKENISED ASSETS AND DIGITAL OWNERSHIP

Tokenised assets represent a paradigm shift in the financial markets, leveraging blockchain technology to convert tangible and intangible assets into digital tokens that can be fractionally owned, transferred, and traded. This revolution has fundamentally changed the idea of ownership, enforcement, and regulation in financial and legal systems across the globe.[23]

A. ROLE OF BLOCKCHAIN IN TOKENISATION

Blockchain technology is the bedrock of tokenized assets, providing a secure, immutable, and decentralized system for recording ownership and transactions.[24] Unlike traditional assets, the blockchain technology is not reliant on banks, clearinghouses, or government registries to verify and transfer ownership; rather, it enables peer-to-peer transactions using cryptographic security.[25]Each tokenized asset is represented as a digital token on a blockchain, which can be programmed with specific legal rights and obligations, making transactions more efficient and automated.

A key advantage of utilizing blockchain in tokenization is the immutability that the system provides, ensuring that once ownership records are recorded on the blockchain, they cannot be altered, deleted, or

---

[23] *Supra* note 1, at 2.

[24] CTR. OF EXCELLENCE IN BLOCKCHAIN TECH., NAT'L INFORMATICS CTR., MINISTRY OF ELECS. & INFO. TECH., BLOCKCHAIN TECHNOLOGY, https://blockchain.gov.in/home/blockchain?blockchain=blockchain.

[25] Shi Dong, Khushnood Abbas, et al., *Blockchain Technology and Application: An Overview*, 9PEERJ COMPUT. SCI. 4 (2023).

tampered with. This intrinsic character of the blockchain technology, significantly reduced risks of fraud, forgery, and double-spending, as every transaction is time-stamped and cryptographically secured within a distributed ledger.[26] Unlike traditional asset registries, blockchain operates on a decentralized consensus mechanism, where the transactions must be verified and validated by a network of nodes before they are appended to the ledger.[27] This procedure eliminates single points of failure and enhances trust and security in asset transactions. Further, the transparency provided by the blockchain system,[28] allows participants and owners to track the history of any tokenized asset, in real time, ensuring that ownership claims are verifiable and indisputable. This feature is especially beneficial in industries where counterfeit products, fraudulent ownership claims, and lack of transparency have been persistent issues, such as real estate, luxury goods, and art markets. Blockchain also simplifies fractional ownership of assets, meaning high-value assets such as real estate, fine art, commodities, and corporate shares can be divided into smaller, tradable digital units[29]. Traditionally, ownership of these assets has been restricted to high-net-worth individuals due to the massive capital requirements and liquidity constraints; however, tokenization lowers the entry barrier by enabling

---

[26] Shi Dong, Khushnood Abbas, et al., *Blockchain Technology and Application: An Overview*, 9PEERJ COMPUT. SCI. 20 (2023).

[27] *Id.*

[28] Mohd Javaid *et al.*, *A Review of Blockchain Technology Applications for Financial Services*, 2 BENCH COUNCIL TRANSACTIONS ON BENCHMARKS, STANDARDS & EVALUATIONS 4 (2022).

[29] WORLD ECONOMIC FORUM, *DIGITAL ASSETS, DISTRIBUTED LEDGER TECHNOLOGY, AND THE FUTURE OF CAPITAL MARKETS* 7 (2023), https://www.weforum.org/reports/digital-assets-distributed-ledger-technology-and-the-future-of-capital-markets/; *See also,* BANK FOR INT'L SETTLEMENTS, *ANNUAL ECONOMIC REPORT 2023* 87 (2023), https://www.bis.org/publ/arpdf/ar2023e.pdf.

individuals to purchase fractional shares of assets, increasing market participation and democratizing investment opportunities.[30]

Regulatory authorities face challenges in monitoring and enforcing compliance in tokenized assets, as these assets can be transferred across borders without a centralized oversight, which raises concerns relating to money laundering, consumer identification, and taxation laws.[31] Since blockchain transactions provide pseudo-anonymity, individuals or entities can execute high-value transactions without undergoing identity verification or financial reporting requirements, making it easier to facilitate illicit financial activities such as money laundering,[32] terrorist financing,[33] and tax evasion.[34] It is legally mandatory for the traditional financial institutions to conduct customer due diligence, transaction monitoring, and suspicious activity reporting to detect and prevent fraudulent activities. However, this centralized monitoring mechanism is absent generally from the blockchain-based assets. Nevertheless, the ecosystem is not devoid of monitoring, and there are several jurisdictions, namely, the European

---

[30] INT'L INST. FOR SUSTAINABLE DEV., *TOKENIZATION OF INFRASTRUCTURE: A BLOCKCHAIN-BASED SOLUTION TO FINANCING SUSTAINABLE INFRASTRUCTURE* 15 (2019).

[31] Mohd Javaid, Abid Haleem, *et al.*, *Tokenized Assets in a Decentralized Economy: Balancing Efficiency, Value, and Risks*, 282 INT'L J. PROD. ECON. 4, 8, 11 (2025).

[32] Adam Turner and Angela Samantha Maitland Irwin, *Bitcoin Transactions: A Digital Discovery of Illicit Activity on the Blockchain*, 25J. FIN. CRIME 109 (2017).

[33] TRM LABS, *2025 CRYPTO CRIME REPORT: KEY TRENDS THAT SHAPED THE ILLICIT CRYPTO MARKET IN 2024* 9 (2025); *See also* U.S. GOV'T ACCOUNTABILITY OFF., *BLOCKCHAIN: EMERGING TECHNOLOGY OFFERS BENEFITS FOR SOME APPLICATIONS BUT FACES CHALLENGES* 31 (2022).

[34] *Supra* note 22, at 5.

Union under the Markets in Crypto-Assets ("**MiCA**") Regulations[35] and the U.S. Financial Crimes Enforcement Network, that have proposed stringent regulations for crypto service providers; enforcement remains challenging due to global inconsistencies in regulatory approaches.[36] Further, taxation laws are difficult to implement, as assets on the blockchain are moved across jurisdictions instantly, making it harder for the authorities to track capital gains, enforce reporting obligations, and prevent tax evasion.[37] A lack of a standardised global tax framework for tokenised assets further complicates compliance, necessitating international cooperation among financial regulators to establish harmonised reporting mechanisms, strict regulatory oversight, and measures for enforcing cross-border compliance in the evolving landscape of tokenised securities.

B. LEGAL RECOGNITION OF DIGITAL OWNERSHIP: PROPERTY RIGHTS VS. SECURITIES LAWS

Classification of tokenised assets is a major challenge in the tokenised asset regulation, as this classification plays a substantial role in determining ownership rights, taxation policies, and regulatory obligations. Traditionally, ownership of physical assets, intellectual property, and financial securities is documented and enforced through centralised registries, contractual agreements, and statutory protections. However, tokenised assets operate in a decentralised digital arena, where assets are

---

[35] *Supra* note 12, at 3.

[36] FIN. CRIMES ENF'T NETWORK, *ADVISORY ON ILLICIT ACTIVITY INVOLVING CONVERTIBLE VIRTUAL CURRENCY* (2019); *See also* Asif Khan *et al.*, *Regulatory Strategies for Combatting Money Laundering in the Era of Digital Trade*, 28 J. MONEY LAUNDERING CONTROL 414 (2025).

[37] *Supra* note 21, at 3.

recorded on blockchain networks rather than physical registries, making it difficult to apply existing legal mechanisms. Further, unlike traditional assets, tokenised assets can be fractionalized,[38] transferred instantaneously across borders, and encoded with smart contracts that define their functionality. This novel concept of assets challenges various legal principles, and whether these assets would be categorised as property, securities, or commodities, as different classifications lead to different regulatory requirements and investor protections. For instance, if a tokenised asset on the blockchain represents ownership in real estate, should it follow real estate laws, or should it be classified as a security because it allows investors to profit from rental income and value appreciation? Such cases directly contradict the established classification of assets.

Regulators have attempted to categorise tokenised assets under existing securities laws, especially if they meet the criteria outlined in the legal principles, such as the Howey Test,[39] as devised in the United States. The Howey Test determines whether an asset qualifies as a security by assessing whether it involves an investment of money in a common enterprise with an expectation of profits derived from the efforts of others.[40] If a tokenised satisfies the requirements under this test, it falls directly under financial regulations, further requiring compliance with

---

[38] PRICE WATER HOUSE COOPERS, *DIGITAL ASSETS—AN EMERGING TREND IN CAPITAL MARKETS* 3, 7 (2022).
[39] Sec. & Exch. Comm'n V. W.J. Howey Co., 328 U.S. 293 (1946).
[40] *Id.*

registration requirements, investor protection laws, and disclosure obligations imposed by financial regulators such as the Securities and Exchange Commission in the United States. Similarly, the European Union, through its MiCA Regulation[41] seeks to create a foundational framework for the classification of tokenised assets, ensuring that they are subject to appropriate investor safeguards.

Classification of tokenised assets, as property, subjects it to property law, real estate law, or intellectual property law, depending on the nature of the underlying asset. However, there is a lack of uniform property laws across jurisdictions, and the majority of the countries at this point do not recognise blockchain-based property registries as legally enforceable ownership records. India till April 2025, has not given any clarification on this aspect, there are no directions issued either by the Central Government, The Reserve Bank of India, or the Securities and Exchange Board of India. The absence of global uniformity and standardisation creates uncertainty for investors, financial institutions, and regulators, particularly when dealing with cross-border transactions involving tokenised real estate, commodities, or other digital assets. Without standardised legal frameworks and regulatory consistency, the market for tokenised assets risks being fragmented, with investors and businesses struggling to navigate overlapping, conflicting, or outdated legal frameworks, potentially stifling innovation and mainstream adoption of tokenised financial instruments.

[41] *Supra* note 11, at 3.

III. GLOBAL REGULATORY APPROACHES TO TOKENISED ASSETS

Tokenised assets have gained prominence in global financial markets; understanding the legal and regulatory approaches of the leading economies is critical to ensure compliance, financial stability, and investor protection. The United States, the European Union, and India represent three contrasting regulatory landscapes; each jurisdiction has taken a unique approach to governing tokenised securities, commodities, and financial instruments. A comparative study of these nations provides a holistic understanding of how distinct regulatory approaches shape the financial, operational, and legal landscape of tokenised assets. Since blockchain-based assets operate across borders, acknowledging the strengths, limitations, and gaps in various legal frameworks is essential for ensuring compliance and financial stability. A comparative analysis of these jurisdictions will help pave the way for a potential global standard for tokenised securities. It will also enlighten policymakers, financial institutions, and legal experts to design effective laws that balance technological innovation with investor protection and financial security.

A. UNITED STATES: A FRAGMENTED YET ROBUST REGULATORY LANDSCAPE

The United States possesses one of the most complex and multifaceted regulatory frameworks for financial assets, which includes tokenised assets, because of the presence of multiple federal and state agencies exercising oversight. The Securities and Exchange Commission

("**SEC**") plays a significant role in regulating the tokenized assets that qualify as securities under U.S. law. The Commission applies the Howey Test,[42] derived from a 1946 Supreme Court case, as previously discussed. If a tokenised asset satisfies the criteria of the test, it is then subjected to rigorous compliance requirements, including securities registration, investor disclosures, anti-fraud protections, and periodic reporting obligations under the Securities Act of 1933[43] and the Securities Exchange Act of 1934.[44] The Commission has routinely pursued enforcement actions against institutions offering unregistered securities as Initial Coin Offerings and Security Token Offerings, leading to legal uncertainty for businesses and investors in the tokenized asset space. Concurrently, the Commodity Futures Trading Commission ("**CFTC**") regulates the tokenised derivatives, digital commodities, and futures contracts, asserting regulatory authority over tokenised assets that qualify as commodities rather than securities.[45] This dual oversight structure creates ambiguity, as some assets may fall into both SEC and CFTC jurisdictions, leaving businesses struggling to navigate compliance requirements effectively. Alongside the Securities and Exchange Commission and Commodity Futures Trading Commission, the federal banking regulators also play a significant role in modeling the regulatory landscape for tokenized assets. The Office of the Comptroller of the Currency, which regulates the national banks and

---

[42] *Supra* note 39, at 8.
[43] Securities Act of 1933, Pub. L. No. 73-22, 48 Stat. 74.
[44] Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 881.
[45] *See, Bd. of Trade of Chi. v. SEC, 677 F.2d 1137, 1142 (7th Cir. 1982). Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities. See,* In re Coinflip, Inc., CFTC No. 15-29 (Sept. 19, 2015).

federal savings associations, has issued direction allowing banks to provide custody services for digital assets, marking a shift towards a greater institutional involvement in the tokenized finance sector.[46]

However, the regulation's enforcement remains fragmented, with state-level laws adding complexities to an already over-burdened system, such as New York's BitLicense framework.[47] Several state-level laws have introduced crypto-friendly policies, while others have imposed strict licensing and compliance requirements, highlighting a nationwide regulatory inconsistency. Further, there is a lack of concrete guidelines for the taxation of tokenised assets, as different authorities, namely, the Internal Revenue Service and the Financial Crimes Enforcement Network, have issued contradictory rules on tax reporting and anti-money laundering obligations.[48] The lack of a uniform federal legal framework has led to regulatory uncertainty, causing businesses and investors to rely on a patchwork of agency rulings, enforcement actions, and state-level laws. However, there have been certain legislative efforts in this direction, such as, Token Taxonomy Act[49] and the Digital Commodities Consumer Protection Act,[50] which were introduced to bring clarity to tokenized asset

---

[46] Office of the Comptroller of the Currency, *Letter Addressing Certain Crypto-Asset Activities*, Interpretive Letter No. 1183 (Mar. 2025).
[47] N.Y. COMP. CODES R. & REGS. tit. 23, pt. 200 (2025).
[48] Peter D. Hardy *et al.*, *IRS Unveils Broad Draft Information Reporting Form for Digital Asset Transactions*, MONEY LAUNDERING WATCH (Apr. 23, 2024), https://www.moneylaunderingnews.com/2024/04/irs-unveils-broad-draft-information-reporting-form-for-digital-asset-transactions/.
[49] Token Taxonomy Act of 2021, H.R. 1628, 117th Cong. (2021).
[50] Digital Commodities Consumer Protection Act of 2022, S. 4760, 117th Cong. (2022).

regulations, yet there is no comprehensive federal legislation governing tokenized assets, leaving the U.S. regulatory landscape for tokenized assets in a state of flux.

B. EUROPEAN UNION: A UNIFIED YET STRINGENT FRAMEWORK

The European Union has taken a structured and proactive approach to regulate tokenised assets through the Markets in Crypto-Assets Regulation,[51] which aims to create a harmonised legal framework across all 27 member states. The Regulations are a landmark initiative created to provide legal certainty and investor protection while ensuring financial stability and compliance with anti-money laundering regulations. Unlike the fragmented approach seen in the United States, where different agencies regulate different aspects of tokenised assets, the EU Regulation establishes comprehensive guidelines that clearly define and categorise various forms of crypto-assets, including utility tokens, stablecoins, and security tokens. Under the regulation, issuers, exchanges, and custodians must obtain licenses from regulatory authorities and adhere to strict operational and transparency standards to protect investors.[52] The framework further imposes liquidity and reserve requirements on stablecoin issuers to mitigate the risks of financial instability.[53] The biggest achievement of this regulation is that it offers a single regulatory framework across the EU, allowing businesses and investors to operate under uniform rules, reducing regulatory arbitrage and increasing cross-border market efficiency.

---

[51] *Supra* note 11, at 3.
[52] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets, 2023 O.J. (L 150) 40.
[53] *Id.*

However, concerns remain with regard to how effectively national regulators will implement and enforce these regulations, given that member states have historically adopted varying interpretations of financial laws. Additionally, emerging tokenised financial instruments, such as decentralised finance and non-fungible tokens, are not fully covered under MiCA, raising concerns that the regulation may become obsolete as blockchain technology evolves.

Additionally, data privacy laws, particularly the General Data Protection Regulation ("**GDPR**"),[54] present substantial legal challenges for tokenised asset markets. The Data Protection Regulation establishes the principle that individuals have the right to control their personal data, including the "right to be forgotten,"[55] which allows users to request the deletion of their personal information. However, the very nature of blockchain technology, directly contradicts the regulation due to its immutable nature.[56] This creates further challenges for institutions and organisations dealing with tokenised assets, to find ways to adopt and implement the regulation without violating the fundamental nature of blockchain. For instance, while hashing or encrypting personal data might offer a potential solution, regulators have yet to determine whether these approaches fully satisfy GDPR requirements. Furthermore, the regulation

---

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[55] Regulation (EU) 2016/679, art. 14, 2016 O.J. (L 119) 1.

[56] PANEL FOR THE FUTURE OF SCI. & TECH., EUR. PARLIAMENTARY RSCH. SERV., *BLOCKCHAIN AND THE GENERAL DATA PROTECTION REGULATION: CAN DISTRIBUTED LEDGERS BE SQUARED WITH EUROPEAN DATA PROTECTION LAW?* 6 (2019).

has strict cross-border data transfer rules, which further complicates the transfer of tokenised assets globally, particularly when dealing with nations outside the EU that have lenient data protection laws.[57]

The Markets in Crypto-Assets Regulation, provides a clear regulatory path for tokenised assets, but the inherent contradiction between the GDPR and the Blockchain technology remains unsolved. Further focus on a centralised regulatory oversight raises concerns that over-regulation could stifle innovation in decentralised finance, making it arduous for blockchain startups and fintech firms to compete with established financial institutions.

C. INDIA: A CAUTIOUS BUT EVOLVING REGULATORY APPROACH

India has taken a cautious approach in order to protect market stability, but has also taken measures to integrate tokenised assets into the financial system, seeking to balance technological innovation, financial stability, and consumer protection. The SEBI is yet to introduce a comprehensive legal framework for tokenised securities, but it has been actively monitoring developments in digital finance.[58] The Board has explored the potential adoption of distributed ledger technology in securities trading, especially to enhance settlement and clearing processes, but formal regulations regarding the issuance, trading, and governance of

---

[57] PANEL FOR THE FUTURE OF SCI. & TECH., EUR. PARLIAMENTARY RSCH. SERV., *BLOCKCHAIN AND THE GENERAL DATA PROTECTION REGULATION: CAN DISTRIBUTED LEDGERS BE SQUARED WITH EUROPEAN DATA PROTECTION LAW?* 90 (2019).

[58] Navdeep Singh, *SEBI Considers Regulatory Role in Crypto Trading, Diverging from RBI's Approach*, ECON. TIMES (May 17, 2024), https://economictimes.indiatimes.com/markets/cryptocurrency/sebi-considers-regulatory-role-in-crypto-trading-diverging-from-rbis-approach-heres-what-experts-think/articleshow/110201982.cms.

tokenised securities remain absent. Meanwhile, the Reserve Bank of India, has traditionally taken a restrictive stance on digital assets due to concerns over financial stability, money laundering, and consumer protection,[59] the Reserve Bank has issued numerous warnings regarding the risks associated with cryptocurrencies and, in 2018, even banned banks from facilitating crypto transactions, a restriction that was later overturned by the Supreme Court of India in 2020.[60] Despite this conservative approach, the Reserve Bank felicitated the launch of India's Central Bank Digital Currency, the Digital Rupee, which indicates a growing institutional acceptance of blockchain-based financial instruments.[61] The introduction of state-backed digital currency suggests that regulators acknowledge the potential benefits of tokenisation, but are wary of privately issued digital assets due to concerns over their volatility, regulatory evasion, and potential use in illicit activities. However, the absence of a specific legal framework governing tokenised securities, commodities, and real estate creates a regulatory vacuum that leaves businesses and investors uncertain about compliance requirements and legal protections.

India's tokenised asset market faces a significant regulatory challenge, that is, the taxes imposed on digital assets, which have substantially impacted liquidity and participation by retail investors. In 2022, the Indian government introduced a 30% tax on crypto transactions,

---

[59] RESERVE BANK OF INDIA, *RBI Cautions Users of Virtual Currencies Against Risks*, https://rbi.org.in/commonman/English/scripts/PressReleases.aspx?Id=2522.
[60] Internet & Mobile Ass'n of India v. Reserve Bank of India, AIR 2021 SC 2720.
[61] *Supra* note 15, at 3.

treating digital assets as speculative investments rather than legitimate financial instruments.[62] Additionally, the government imposed a 1% Tax Deducted at Source on all crypto trades, making high-frequency trading and liquidity provision less attractive for institutional and retail investors.[63] These policies have raised concerns that tokenised assets could also face similar compliance burdens, deterring businesses from engaging in blockchain-based finance. Further, the lack of a comprehensive law for tokenised assets significantly affects market participation and creates a sense of uncertainty with regard to ownership rights, transferability, and dispute resolution.

An explicit legal recognition of tokenised assets could help businesses in exploring a tokenisation model for the masses; however, at present, businesses face challenges in securing institutional funding, regulatory approvals, and consumer trust. Additionally, India's regulatory environment is significantly influenced by global trends, and as the European Union and the United States establish clearer tokenisation regulations, India faces increasing pressure to legislate on the subject matter. Policymakers must strike a delicate balance between fostering financial innovation and ensuring compliance with investor protection laws. The lack of a structured legal framework remains one of the biggest obstacles to the growth of India's tokenised asset industry, and regulatory clarity will be essential for businesses, banks, and investors looking to leverage blockchain technology for asset digitisation and financial inclusion.

---

[62] Finance Act, No. 6 of 2022, § 115BBH (India).
[63] Finance Act, No. 6 of 2022, § 194S (India).

IV. KEY CHALLENGES IN INTEGRATION OF BANKING AND TOKENISED ASSETS

Tokenised assets have become increasingly integrated into the global financial markets; however, they present significant challenges for banks, regulators, and investors. While tokenisation provides benefits such as enhanced liquidity, efficiency, and transparency, it also raises complex legal, operational, and financial risks. Traditional banking systems were built and have operated on the trust of their customers, and have long served as the custodians and intermediaries of financial assets. These institutions now must now navigate uncertain regulatory environments, security vulnerabilities, and compliance burdens when dealing with digital asset custody, trading, and transactions. The lack of harmonised global regulations further creates cross-border challenges, making it difficult for banks to establish clear compliance frameworks and regulations. This section addresses and examines the key challenges inherent to the integration of tokenised assets into traditional banking systems.

A. REGULATORY UNCERTAINTY AND COMPLIANCE RISKS

The primary obstacle in the integration of banking and tokenised assets is the lack of a uniform regulation, especially with regard to the classification of tokenised assets, under the current financial regulations. The legal definition of a tokenised asset is ambiguous across jurisdictions, where some regulators classify them as securities, while others have classified them as commodities, property, or even unregulated digital assets.

B. CUSTODY AND SECURITY CONCERNS

Tokenised assets require secure storage solutions, and banks must decide whether to offer custodial or non-custodial services to the investors. Custody models significantly impact regulatory obligations, security measures, and liability risks, making them a critical challenge in banking and tokenised asset management.

i. Custodial v. Non-Custodial Services

Traditional banks function by holding physical and digital financial assets on behalf of clients, acting as custodians to ensure security and regulatory compliance. However, blockchain-based assets can function on non-custodial measures as well, where the owners of the assets control their private keys and funds without depending on intermediaries. This poses significant challenges for traditional banks, as they are now required to develop infrastructure for digital asset custody, while complying with regulatory obligations, and addressing concerns with regards to security breaches.[64]

ii. Cybersecurity and Financial Stability Issues:

Tokenised assets are vulnerable to hacks, fraud, and cyberattacks, raising concerns about financial security and stability.[65] Major financial institutions have struggled with cybersecurity threats while offering digital asset services. Unlike traditional financial services, where banks can directly reverse fraudulent transactions, blockchain transactions are irreversible, by

---

[64] Radoslaw Ignatowicz & Alfred Taudes, *Opportunities in Digital Assets and Digital Custody: Tracking the Modernisation of Standard Custody Offering*, 15 J. SEC. OPERATIONS & CUSTODY 199, 200, 202 (2023).

[65] *Id.*

their very nature, meaning stolen assets are nearly impossible to recover.[66] The exposure puts banks at reputational risks, compliance issues, and potential lawsuits if they fail to secure client assets effectively.

C. BANK COMPLIANCE AND FRAUD PREVENTION

Tokenised assets face a major risk, which is the potential use in money laundering,[67] terrorist financing, and fraudulent schemes. Traditional banking systems are bound by strict Anti-Money Laundering and Know Your Customer regulations, as tokenised transactions can be executed anonymously or pseudonymously, making it difficult for regulators and banks to track illicit financial activities.

i. Risks of Money Laundering and Fraudulent Transactions

Criminal organisations have reportedly used tokenised assets, decentralised exchanges, and digital currencies to move funds across jurisdictions to fund their activities without regulatory oversight. The pseudo-anonymous character of blockchain technology makes it strenuous to trace the source of illicit funds, further increasing concerns over terrorist financing, tax evasion, and fraud.[68] To prevent this, financial watchdogs like the Financial Action Task Force have introduced the "Travel Rule,"

---

[66] *Supra* note 25, at 6.
[67] M. C. Mehanathan, *LAW ON PREVENTION OF MONEY LAUNDERING IN INDIA* 24–25 (LexisNexis India, 3d ed. 2022).
[68] *Supra* note 29, at 7.

requiring banks and crypto service providers to collect customer information for digital asset transactions.[69]

ii. Bank Obligations

Banks are mandated to implement stringent Anti Money Laundering and Know Your Customer measures, which include identity verification, transaction monitoring, and suspicious activity reporting. However, in the case of tokenised assets, verifying ownership and tracking transactions is highly complex, attributable to the decentralised nature of the blockchain networks.[70] To combat this, regulators are heavily pushing for the banks to develop and integrate on-chain compliance tools, which function on the fusion of blockchain analytics and AI-powered transaction monitoring to detect suspicious activities in real time.[71] However, these compliances further increase operational costs for the banks and create regulatory burdens for banks entering the digital asset sector.

D. CONSUMER PROTECTION AND FINANCIAL INCLUSION

Tokenised assets offer modern investment opportunities, but they also introduce the risk for retail investors, especially those who are not familiar with the blockchain system. Ensuring consumer protection and financial inclusion is essential to establish trust of the general public in the tokenized financial system.

---

[69] FIN. ACTION TASK FORCE, *INTERNATIONAL STANDARDS ON COMBATTING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS*16 (2012).

[70] *Supra* note 29, at 6.

[71] Esman Kurum, *RegTech Solutions and AML Compliance: What Future for Financial Crime?*, 30 J. FIN. CRIME 790 (2023).

i. Retail Investor Risks and Market Manipulation

The majority of retail investors lack knowledge about tokenised assets, making these individuals vulnerable to fraud, market manipulation, and investment losses. The rise of pump-and-dump schemes, flash loan attacks, and rug pulls in crypto-based assets has underscored the need for strict regulatory safeguards.[72] Attributing to the absence of proper safeguards and regulations, unscrupulous actors may exploit loopholes to engage in fraudulent activities, leaving investors with little legal recourse.[73]

ii. Ensuring Secure Access for Consumers Through Banks

Banks have a significant part in providing investors with safe and secure access to tokenised assets through regulated platforms and establishing secure custody solutions. Through the integration of tokenised assets into the traditional and mainstream financial system, the associated institutions could reduce risks associated with decentralised finance, while expanding financial inclusion. Tokenisation allows retail investors to participate, markets such as real estate, fine art, and private equity, which have historically been limited only to wealthy individuals.[74] However, ensuring that all investors have equitable access to secure, regulated tokenised asset markets remains a challenge, requiring collaborative efforts from banks, policymakers, and financial regulators.

---

[72] INT'L ORG. OF SEC. COMM'NS, *INVESTOR EDUCATION ON CRYPTO-ASSETS* 54 (2024).
[73] *Id.*
[74] *Supra* note 7, at 2.

The rise of tokenised assets tender opportunities alongside novel challenges for the banking industry, compelling organisations to adapt to the new regulatory, security, and compliance requirements. The absence of a uniform global legal framework, in addition to cybersecurity threats, anti-money laundering and know your customer compliance burdens, and investor protection risks must be addressed to successfully achieve the successful integration of tokenised assets into the traditional financial systems. Regulatory measures are essential to assist banks in successfully navigating through these complexities and to shape the future of tokenised finance.

V. REAL-LIFE CASE STUDIES ON TOKENISED ASSETS AND BANKING LAW

The decentralised nature of blockchain has disrupted traditional financial systems, raising complex legal and regulatory issues related to ownership, compliance, security, and jurisdictional oversight. Understanding the approaches taken by different jurisdictions and institutions to address these challenges is critical for creating an effective regulatory framework to ensure market stability. Real-world case studies provide invaluable insight into legal challenges, enforcement measures, compliance strategies, and policy responses, that have influenced the development of tokenised assets across the globe. These real-life instances offer crucial insights for the regulators, financial institutions, and investors navigating the rapidly evolving world of tokenised finance.

A. SEC VS. RIPPLE[75] (XRP): THE SECURITIES CLASSIFICATION DEBATE

The SEC filed a lawsuit against Ripple Labs Inc., alleging that the company had offered unregistered securities in the open market by selling XRP tokens. The Commission claimed that XRP met the required criteria of an "investment contract" under the Howey Test, as established by the Supreme Court of the United States.[76] The Commission submitted that Ripple had made sufficient efforts for the promotion of XRP, which led the investors to expect profits, subjecting the token to be registered as a security with the Commission, and to comply with the applicable security laws.

The SEC was strongly opposed by Ripple, submitting that XRP should not be classified as a security, but as a digital currency, similar to Bitcoin and Ethereum. Further submitting that XRP serves as a medium of exchange for cross-border payments, rather than functioning as an investment contract. It was also pointed out that the Commission has already classified Bitcoin and Ethereum as non-securities, which led to an inconsistent application of regulations. Ripple also submitted that XRP had been traded on exchanges for years to the lawsuit, and the company had received no preliminary warnings. The lawsuit had significant consequences for XRP and Ripple, as major cryptocurrency exchanges delisted XRP,

[75] SEC. & EXCH. COMM'N v. Ripple Labs, Inc., 697 F. Supp. 3d 126 (S.D.N.Y. 2023).
[76] *Supra* note 39, at 8.

causing its market value to plummet and raising significant concerns over the irregular application of laws on the classification of digital assets.

The case had far-reaching implications for the regulation of tokenised assets in the United States. The decision not only influences the classification of cryptocurrencies but also significantly impacts the future of banking and financial services in the blockchain system. If the Commission had succeeded with its submission, it would have set a precedent which would have required all the crypto-issuing agencies to register their tokens as securities, substantially increasing the compliance burdens and limiting token liquidity, the decision would have also impacted banks and financial institutions and their ability to provide custodial services for tokenised assets, as cryptocurrencies being classified as securities would have led to imposition of strict banking regulations and reporting requirements. Further, all the blockchain-based exchange platforms would have had to register with the commission, leading to higher operational costs and potential delisting of tokens classified as securities.

However, the Supreme Court took a contrasting decision, where XRP was not classified as a security, providing relief to the crypto industry. The decision highlighted the fact that not all digital assets would be classified as securities, addressing the concerns of an overly aggressive regulatory crackdown. However, the ruling still left uncertainties, as XRP was classified as a security when sold directly to institutional investors, underscoring the need for a comprehensive regulatory framework. This case has further intensified demands for legislative clarity, with

policymakers debating the necessity of new crypto-specific regulations that distinguish between securities, commodities, and digital currencies.

B. BNY MELLON'S CRYPTO CUSTODY SERVICES

BNY Mellon, the world's largest custodian bank, in 2021, made a significant stride in the digital asset market by launching its digital asset custody platform, the first major U.S. bank to offer crypto-based custody services to its customers.[77] BNY Mellon is a systemically important financial institution,[78] its entry into the crypto arena marks a significant milestone for institutional adoption of digital assets. The bank's decision to offer custody services for Bitcoin and Ethereum, in addition to traditional financial assets, highlights the growing demand from institutional investors for secure and regulated solutions to manage their tokenised holdings. The bank's decision to act as a custodian for digital assets is motivated by the rising acceptance of tokenised assets. This initiative is aligned with the evolving role of banks in the blockchain ecosystem, where financial institutions are expected to facilitate and safeguard digital transactions. This move has positioned BNY Mellon as a pioneer among the traditional banks in the realm of digital asset integration, bridging the gap between traditional and decentralised finance.

The entry into the crypto custody market required BYN Mellon to navigate a complex system of financial regulations and secure the necessary

---

[77] BNY Mellon Launches New Digital Asset Custody Platform, BNY MELLON, https://www.bny.com/corporate/global/en/about-us/newsroom/press-release/bny-mellon-launches-new-digital-asset-custody-platform-130305.html.

[78] FIN. STABILITY BD., *2024 LIST OF GLOBAL SYSTEMICALLY IMPORTANT BANKS (G-SIBS)*, https://www.fsb.org/2024/11/2024-list-of-global-systemically-important-banks-g-sibs/.

approvals from the appropriate authorities. The bank operated closely with the Office of the Comptroller of the Currency, which had previously issued a direction in 2020 allowing national banks to offer crypto custody services.[79] The bank had to address numerous compliance requirements, such as anti-money laundering, know your customer, as the Financial Crimes Enforcement Network had imposed stringent rules on banks to implement robust transaction monitoring and reporting mechanisms to address suspicious activities in the crypto space.[80] Further, the bank also had to address cybersecurity risks and operational resilience, as digital asset custody requires advanced security protocols to prevent hacks, unauthorised access, and fraud. The bank installed a multi-layered security infrastructure, including multi-signature authentication and blockchain forensic tools, to enhance transaction security.[81] Despite these efforts, the regulatory uncertainty surrounding financial assets in the United States continues to be an issue. Nevertheless, the successful launch of regulated digital asset custody services by BNY Mellon has the potential to act as a blueprint for other financial institutions, demonstrating the role of traditional banks in the secure and compliant adoption of tokenised assets.

---

[79] *Supra* note 48, at 10.
[80] *Supra* note 36, at 7.
[81] BNY Mellon Forms New Digital Assets Unit to Build Industry's First Multi-Asset Digital Platform, BNY MELLON, https://www.bny.com/corporate/global/en/about-us/newsroom/press-release/bny-mellon-forms-new-digital-assets-unit-to-build-industrypercent27s-first-multi-asset-digital-platform-130169.html.

C. THE DAO HACK: SMART CONTRACT VULNERABILITIES AND LEGAL ACCOUNTABILITY

The Decentralised Autonomous Organisation ("**DAO**") was launched on the Ethereum blockchain in 2016 as an experimental decentralised venture capital fund, which allowed investors to pool funds and collectively vote on the projects to be funded. The Organisation raised over $150 million in ETH, becoming one of the most ambitious blockchain-based projects at the time. However, there was a critical flaw in the smart contract code,[82] which allowed an attacker to exploit a re-entrancy vulnerability, allowing repeated withdrawals of funds before the contract updated the balance. This led to the theft of about $60 million worth of ETH, creating one of the largest controversies in blockchain history.[83] This attack exposed the critical weaknesses in smart contract security and governance, especially the risks associated with immutable and self-executing contracts. Unlike traditional contracts, which heavily rely on legal enforcement and amendments, smart contracts are executed automatically without any centralised oversight or intervention. This hack raised significant legal issues about accountability and enforceability of smart contracts, but the lack of legislative clarity left investors with no immediate legal recourse, as traditional laws did not cover disputes arising from autonomous code execution.

---

[82] Izhar Mehar *et al.*, *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack January 2019*, 21 J. CASES ON INFO. TECH. 28 (2019).
[83] *Id.*

The Ethereum community, in response to the hack, was in a legal and ethical dilemma, whether to let the blockchain remain immutable or intervene to recover lost funds. Ultimately, the developers implemented a hard fork,[84] which meant rewriting all of the transactions on the blockchain, throughout its history, to restore the stolen token to its original owners. This event highlighted the lack of concrete legal mechanisms for handling smart contract failures. Further, since blockchain transactions are irreversible, investors had limited legal recourse, exposing the risks of relying on code as law. The incident also underscores the need for security audits, formal verification of smart contracts, and legal safeguards to protect investors from unforeseen vulnerabilities. To prevent such incidents in the future, regulators and blockchain developers must collaborate to create standardised legal frameworks that balance automation with investor protection. This includes establishing legal accountability for smart contract failures, dispute resolution mechanisms, and enforceable security standards to prevent similar cases in the future.

VI. POLICY RECOMMENDATIONS FOR THE ADOPTION OF DECENTRALISED FINANCE

Tokenised assets will continue to reform global financial markets; therefore, regulatory frameworks must also evolve to address the emerging while fostering innovation. The rapid expansion of blockchain technology has prompted policymakers to anticipate future legal developments and implement reforms that balance market growth with regulatory oversight.

[84] Simona Ramos *et al.*, *A Great Disturbance in the Crypto: Understanding Cryptocurrency Returns Under Attacks*, 2BLOCKCHAIN: RES. & APPLICATIONS2 (2021).

Central banks, financial institutions, and regulators across the globe are now focused on standardising tokenised asset governance and enhancing security measures.

A. THE ROLE OF CENTRAL BANKS IN TOKENISED ASSET REGULATION

Central banks across jurisdictions have a crucial role in shaping the regulatory landscape for tokenised assets.[85]These institutions are the financial backbones of their economies and are tasked with ensuring monetary stability, mitigating systemic risks, and protecting consumers. Central banks across the globe, including the Federal Reserve (U.S.), European Central Bank, and Reserve Bank of India, are actively analysing the implications of tokenised finance on payment systems, monetary policy, and financial stability.[86]

The most significant development in central banking is the issuance of Central Bank Digital Currencies ("**CBDC**"), which aim to transform financial systems by coexisting with tokenised assets, while maintaining regulatory oversight and monetary stability.[87] When compared to decentralised cryptocurrencies, the CBDCs are state-backed digital currencies that leverage blockchain technology to facilitate faster, more

---

[85] BANK FOR INT'L SETTLEMENTS & COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, *TOKENISATION IN THE CONTEXT OF MONEY AND OTHER ASSETS: CONCEPTS AND IMPLICATIONS FOR CENTRAL BANKS* 20 (2024).

[86] *Id.*

[87] *Supra* note 12, at 3.

secure, and cost-efficient transactions.[88] The most significant use case for these currencies is their potential to enhance cross-border payments by reducing reliance on intermediary banks, lowering remittance costs, and improving settlement efficiency.[89] Additionally, CBDCs could be used to promote and ensure financial inclusion by providing people without access to traditional banks, direct access to digital financial services without the need for traditional banking infrastructure.[90]

However, the swift adoption of CBDCs raises critical issues, such as privacy, as state-controlled digital currencies could enable greater government surveillance over financial transactions of any person, potentially infringing on individual financial autonomy.[91] Additionally, the CBDCs hold the potential to replace decentralised cryptocurrencies and stablecoins, as CBDCs are state-controlled digital money could diminish the use and relevance of private digital assets.

To address these challenges, central banks are utilising regulatory sandboxes,[92] which are controlled environments where tokenised financial products can be tested under regulatory supervision before general

---

[88] Lambis Dionysopoulos *et al.*, *Central Bank Digital Currencies: A Critical Review*, 91 INT'L REV. FIN. ANALYSIS 4 (2024).

[89] BANK FOR INT'L SETTLEMENTS & COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, *TOKENISATION IN THE CONTEXT OF MONEY AND OTHER ASSETS: CONCEPTS AND IMPLICATIONS FOR CENTRAL BANKS* 10 (2024).

[90] *Supra* note 87, at 22.

[91] Kieran P. Murphy *et al.*, *Central Bank Digital Currency Data Use and Privacy Protection*, IMF FINTECH NOTES 14 (2024); *See also* Jiaying Jiang, *Privacy Implications of Central Bank Digital Currencies*, 54 SETON HALL L. REV. 73 (2023).

[92] G20 BRAZIL, *DIGITAL CURRENCIES IN THE DEVELOPING WORLD: COORDINATING AND SANDBOXING CBDCS* 8 (2024); DEP'T OF ECON. & SOC. AFFS., U.N., *GLOBAL TOOLKIT ON REGULATORY SANDBOX FOR CENTRAL BANK DIGITAL CURRENCY AND FINTECH* 15 (2023).

implementation. These sandboxes allow regulators to assess risks, compliance requirements, and technological feasibility without immediately imposing rigid legal restrictions. Additionally, international initiatives such as the Bank for International Settlements Innovation Hub,[93] aim to develop uniform standards for tokenised finance that are accepted and implemented globally, promoting a harmonised approach to digital asset governance. However, the fundamental challenges, which are striking the right balance between innovation and regulatory control, remain unanswered, as excessive regulation could stifle market growth and discourage financial innovation, a lack of oversight could lead to financial instability, fraud, and systemic risks. Thus, it is the duty of the central banks to collaborate with policy makers, financial institutions, and blockchain developers to ensure that CBDCs and tokenised assets can coexist within a secure, transparent, and well-regulated financial ecosystem that fosters both innovation and consumer protection.[94]

B. RECOMMENDATIONS FOR POLICYMAKERS AND FINANCIAL INSTITUTIONS

To address the complexities surrounding tokenised asset regulation, policymakers and financial institutions must adopt a proactive, collaborative, and adaptive approach. The following recommendations

---

[93] BANK FOR INT'L SETTLEMENTS, *ABOUT THE BIS INNOVATION HUB*, https://www.bis.org/about/bisih/about.htm.

[94] BANK FOR INT'L SETTLEMENTS & COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, *TOKENISATION IN THE CONTEXT OF MONEY AND OTHER ASSETS: CONCEPTS AND IMPLICATIONS FOR CENTRAL BANKS* 11 (2024).

outline strategic measures for ensuring compliance, enhancing security, and fostering innovation in tokenised finance:

i. **Develop Clear Legal Definitions**: Precise legal classifications must be established for the various types of tokenised assets, differentiating between security tokens, utility tokens, stablecoins, and digital property to eliminate regulatory uncertainty.[95]

ii. **Enhance Anti Money Laundering and Know Your Customer Compliance**: Financial institutions must implement blockchain analytical tools and should work towards smart regulations and adoption of regulatory technology, to ensure effective monitoring, risk assessment, and fraud prevention in tokenised transactions.

iii. **Strengthen Smart Contract Governance**: Legal frameworks can introduce guidelines to recognise smart contracts as enforceable legal agreements, ensuring that dispute resolution mechanisms are present for swift disposal of grievances and security audits are in place to mitigate vulnerabilities.

iv. **Encourage Global Regulatory Collaboration**: Governments across the globe should work closely with international financial institutions to introduce standardised regulations, to reduce cross-border legal discrepancies and ensure consistency in compliance standards across jurisdictions.[96]

v. **Support Innovation through Regulatory Sandboxes**: Regulators must encourage financial institutions to participate in the testing of new

---

[95] SEC. & EXCH. COMM'N v. Ripple Labs, Inc., 697 F. Supp. 3d 126 (S.D.N.Y. 2023),
[96] FIN. STABILITY BD., *THE FINANCIAL STABILITY IMPLICATIONS OF TOKENISATION* 13 (2024).

financial products by creating sandbox programs, which allow businesses to experiment with tokenised finance solutions under supervised regulatory conditions, and without affecting the market.

vi. **Improve Consumer Protection Measures**: For a smooth adoption of decentralised assets by the consumers globally, the regulators must implement robust investor protection policies, and ensure that retail investors have access to transparent disclosures, fraud prevention mechanisms, and specialised legal recourse options, which should be made available to the consumers.[97]

vii. **Integrate Tokenised Assets into Traditional Finance**: Banks and financial institutions should explore and implement measures to seamlessly integrate tokenised asset services within existing banking frameworks, such as offering digital asset custody, blockchain-based lending, and smart contract-driven financial products.

VII. CONCLUSION AND OBSERVATION

Tokenised assets continue to reshape traditional financial markets, banking systems, and digital ownership models. It is crucial to examine the legal and regulatory frameworks that govern them. The frameworks of the major economies do not directly address the classification of digital assets, and treat them as securities, commodities, or digital property, without any fixed criteria. The United States, European Union, and India have

---

[97] Georg Lorenz, *Regulating Decentralized Financial Technology: A Qualitative Study on the Challenges of Regulating DeFi with a Focus on Embedded Supervision*, 7 STAN. J. BLOCKCHAIN L. & POL'Y 239 (2024).

demonstrated divergent approaches to tokenized asset regulation. However, the integration of blockchain into the traditional markets is not without concerns, such as anti-money laundering measures, cybersecurity vulnerabilities, and the need for consumer protection. There is a need for greater legal clarity, standardised regulations, and proactive banking sector engagement in the governance of tokenised assets.

The future of tokenised assets in the realm of banking and digital ownership is massively dependent upon the evolution of legal frameworks, technological advancements, and institutional adoption.[98] As an increasing number of financial institutions explore the use cases of tokenised assets, banks are likely to expand custody and transaction services while navigating regulatory uncertainties. Central banks also have a pivotal role to play, as evident from the development of Central Bank Digital Currencies and regulatory sandboxes. From a legal standpoint, a standardised classification of digital assets should be of paramount consideration to eliminate inconsistencies and regulatory arbitrage. Moreover, ensuring robust cybersecurity measures, fraud prevention protocols, and consumer protection laws will be critical to building trust in tokenised financial ecosystems. The role of artificial intelligence and regulatory technology in automating compliance monitoring, fraud detection, and financial reporting is indisputable in shaping the trajectory of tokenised banking services.[99]

---

[98] Mohd. Javaid *et al.*, *A Review of Blockchain Technology Applications for Financial Services*, 2 BENCH COUNCIL TRANSACTIONS ON BENCHMARKS, STANDARDS & EVALUATIONS 11 (2022).

[99] Denise Garcia Ocampo *et al.*, *Crypto, Tokens and DeFi: Navigating the Regulatory Landscape* 41 (Bank for Int'l Settlements 2023).

For the tokenised assets to be adopted by the mainstream markets, the regulatory and legal systems must evolve in tandem with technological advancements.[100] The policymakers must work with the financial regulators and adopt a balanced approach that fosters innovation while ensuring legal certainty and financial stability. While overregulation in this area could hinder growth and drive businesses to less regulated jurisdictions. Insufficient oversight could lead to fraud, security breaches, and financial instability. A coordinated effort is of paramount importance and is required to create a harmonised global regulatory standard to facilitate cross-border transactions and market interoperability. Countries with lucid and unambiguous legal frameworks and investor protection measures will be the leaders in the tokenised financial revolution, which represents a paradigm shift in banking, finance, and digital ownership. However, its full potential can only be realised through adaptive legal frameworks, proactive regulatory measures, and institutional innovation. By examining the existing legal loopholes, enhancing consumer protection measures, and fostering global collaboration, policymakers and financial institutions can ensure that tokenisation strengthens and increases financial inclusion, enhances liquidity, and revolutionises the very basis of how assets are owned, traded, and governed in the digital age.

---

[100] Ying Zhang *et al.*, *Centralized Use of Decentralized Technology: Tokenization of Currencies and Assets*, 71 STRUCTURAL CHANGE & ECON. DYNAMICS23, 24 (2024).

Parth Gupta, *Reframing PN3: Clarifying Beneficial Ownership and Regulatory Oversight in India's Land-Border FDI Policy,* 12(1) NLUJ L. REV. 186 (2026)

REFRAMING PN3: CLARIFYING BENEFICIAL OWNERSHIP AND REGULATORY OVERSIGHT IN INDIA'S LAND-BORDER FDI POLICY

~ Parth Gupta[*]

ABSTRACT

*This article analyses the level of relaxation possible of Press Note 3 ("**PN3**") (2020)'s rigorous standards, the emphasis on government authorization of all investment from land-boarding nations, that can occur without harming national security, especially in non-sensitive industries like as technology and manufacturing. Two urgent regulatory grey areas are at the centre of this investigation: the absence of a clear, predictable clearance system and the imprecise definition of "beneficial ownership," both of which have caused varying interpretations and varying levels of compliance. Moreover, mixed signals from Authorized Dealer ("**AD**") banks regarding pricing and reporting norms make it difficult to execute deals and further muddies the regulatory atmosphere and hence halts or derails cross-border capital flows. As geopolitical tensions, the India-China dynamics and larger US-India trade relations, dictate the course of Foreign Direct Investment ("**FDI**") policy, changes within PN3 can unlock significant investments. However, certainty with regard to thresholds of beneficial ownership and streamlined AD bank processes is necessary both to achieve investor confidence and maintain national security. Using government Standard Operating Procedures ("**SOPs**"), stakeholder input, and*

[*] Parth Gupta is a third-year B.A., LL.B. (Hons.) student at Institute of Law, Nirma University, Ahmedabad

data on approved and rejected proposals, this article puts forward a calibrated regulatory road map of relaxation of PN3's stranglehold on non-sensitive industries.

TABLE OF CONTENTS

I. INTRODUCTION……..188

II. ORIGIN AND LEGAL PRECEDENT TO PRESS NOTE 3 (2020): A BRIEF TIMELINE TO INDIA'S FDI POLICY EVOLUTION.....193

A. THE MOVE TOWARDS STRINGENCY: THE BACKGROUND TO PRESS NOTE 3 (2020) 194

B. LEGAL IMPLICATIONS AND INSTANT EFFECT 196

III. THE REGULATORY LABYRINTH: UNPACKING AMBIGUITIES IN PN3'S IMPLEMENTATION.....198

A. THE OPAQUE APPROVAL FRAMEWORK AND LACK OF PREDICTABILITY.....198

B. BENEFICIAL OWNERSHIP PUZZLE": CONCEPTUALIZING CONTROL OF CROSS-BORDER INVESTMENTS 201

C. THE AD BANK CONUNDRUM: CONFLICTING GUIDANCE AND OPERATIONAL HURDLES.....203

IV. GEOPOLITICAL CROSSCURRENTS: FRAMING FDI POLICY IN A MULTIPOLAR WORLD 205

A. INDIA-CHINA INTERPLAY AND THE NATIONAL SECURITY URGENCY.....206

B. US-INDIA TRADE RELATIONS AND THE BROADER INTERNATIONAL INVESTMENT CLIMATE.....208

V. BUILDING A CALIBRATED ROADMAP OF REGULATIONS: MERGING NATIONAL SECURITY AND INVESTMENT IN NON-SENSITIVE AREAS 210

A. RESTRUCTURING THE APPROVAL SYSTEM: MAKING IT MORE TRANSPARENT AND PREDICTABLE 210

B. DEFINITION OF "BENEFICIAL OWNERSHIP": COMMON DOCTRINAL APPROACH 212

C. STREAMLINING AD BANK PROTOCOLS: INCREASING CONSISTENCY 214

VI. CONCLUSION 216

I. INTRODUCTION

The world economy has observed a distinct trend in the past few years, involving enhanced convergence between national security issues with foreign direct investment regimes.[1] Countries all over the world are reviewing their open investment regimes, commonly establishing stringent screening regimes to protect strategic assets, important infrastructure, and burgeoning industries from perceived dangers created by state-backed or state-controlled foreign entities.[2] India, which is a growing economic giant as well as one of the world's large recipients of global FDI, is no exception to this phenomenon. In April 2020, in the midst of the first wave of the COVID-19 pandemic as well as rising geopolitical tensions, most significantly with China, the Government of India issued PN3.[3]

The PN3 substantially rewrote India's FDI policy to insist on prior government approval for all indirect and direct foreign investments that are from entities or individuals in countries sharing a land border with India, or in which the beneficial owner of an investment is in or is from such countries.[4] While the seeming objective was to avoid opportunistic acquisition of distressed Indian businesses due to economic pressure, the

---

[1] Ioannis Kokkoris, *Merger Control, National Security, and Foreign Direct Investment Screening: A Comparative Perspective, 1st Edition, OXFORD LAW PRO), (4 June 2024)*, https://doi.org/10.1093/law-ocl/9780198837343.001.0001

[2] Lorenzo Bencivelli et al., *The Rise of Foreign Investment Screening in Advanced Economies*, VoxEU.org CEPR (16 Nov 2023), https://cepr.org/voxeu/columns/rise-foreign-investment-screening-advanced-economies.

[3] Press Note No. 3 (2020 Series) *(FDI Policy),* DPIIT, MIN. OF COM. & INDUS., GOV'T OF INDIA (Apr. 17, 2020), https://dpiit.gov.in/sites/default/files/pn3_2020.pdf.

[4] Sandeep Mehta, *India*, Norton Rose Fulbright, (December 2025), https://www.nortonrosefulbright.com/en-us/knowledge/publications/24313880/india

reasons were national security-based.[5] The modification, from the automatic route for these investments, marked a dramatic reversal from India's liberalization of FDI in the previous three decades.

Nonetheless, the application of PN3 has not been without significant challenges, creating a complicated regulatory maze for foreign investors as well as domestic players. The strict parameters, though motivated by legitimate national security considerations, have ironically brought in vital regulatory uncertainties that suppress capital flows as well as dampen investor confidence, specifically in industries that are not immediately related to national security. There are two main issues that are the subject matter of this investigation. *First*, the approval process under PN3 is inflexible as well as unpredictable. The lack of unequivocally defined SOPs, openly available criteria for approval or rejection, as well as clear timelines, has made the process opaque as well as discretionary.[6] *Second*, the definition of "beneficial ownership" in the case of PN3 is radically unclear. Without a standardized as well as explicit threshold level, interpretations are extremely divergent, giving rise to heterogeneous compliance burdens as well as heightening the probability of under-inclusion as well as over-inclusion of investments under the domain of the cognizant restrictive

---

[5] Praveenop, *India's FDI Challenge Amidst Global Realignment* - JICE IAS, (2025), https://jiceias.com/upsc-current-affairs-indias-fdi-challenge-amidst-global-realignment/.

[6] Sumit Parashar, *Factors Affecting FDI Inflow in China and India*, (Univ. of Alberta Working Paper, 2015), https://www.ualberta.ca/en/china-institute/media-library/media-gallery/research/research-papers/fdichinaandindiasumitparashar201507.pdf.

regime.[7] *Third*, adding to these are the inconsistent AD bank guidance notes, issued by pivotal intermediary entities in FDI transactions, which obscure the regulatory landscape as well as slow deal consummation.[8]

While India manages through a complicated geopolitical landscape, the border differences that have persisted in relation to China and a changing American security partnership, the proportionality and effectiveness of its FDI screening regimes are most relevant. Though the need to secure national security is unshakeable, the opportunity to realize significant investments in non-sensitive sectors through a more balanced approach is no less significant. This article suggests that India can, and ought to, ease some stringent provisions of PN3 in non-sensitive sectors whilst still protecting national security objectives.

This article seeks to address key questions as to what extent can India relax PN3 conditions in non-sensitive sectors without national security suffering, how can regulatory uncertainties relating to the approval structure, as well as to the term "beneficial ownership" can be addressed to improve predictability and confidence among investors, and what are the specific revisions to PN3 and AD bank protocols that are needed to strike a prudent balance between national security and investor confidence in non-sensitive sectors.

---

[7] Vikrant Rana & Shantam Sharma, *Significant Beneficial Ownership under the Indian Companies Act: A Legal Guide for Businesses*, S.S. RANA & CO, (August 12, 2025), https://ssrana.in/articles/significant-beneficial-ownership-under-the-indian-companies-act-a-legal-guide-for-businesses/.

[8] Praveenop, *supra* note 5.

In order to address these issues, this article will first scrutinize the origins and regulatory regime of PN3 in the wider framework of India's changing FDI policy. Then, it will critically deconstruct the regulatory confusion relating to the approval regime, the elusive definition of "beneficial ownership," as well as operating obstacles in the form of adverse AD bank guidance. Thereafter, the article will examine the geopolitical currents affecting India's FDI regime, specifically India-China relations and US-India trade ties. Lastly, based on a doctrinal examination, this article will advance a calibrated regulatory plan, involving a specified regime and legal reforms to relax PN3's stranglehold over non-sensitive sectors, thus encouraging increased predictability as well as investor friendliness while protecting legitimate national security concerns.

II. ORIGIN AND LEGAL PRECEDENT TO PRESS NOTE 3 (2020): A BRIEF TIMELINE TO INDIA'S FDI POLICY EVOLUTION

India's transition towards an open economy, began in early 1990s and, featured the slow but steady liberalization of its FDI regime. Until then, India's strategy towards foreign investment tended to be predominantly protectionist with strict controls.[9] The 1991 economic reforms brought with them a new dawn that appreciated FDI as an important stimulant for economic expansion, technology flow, as well as generation of jobs.[10] This liberalization witnessed the gradual elimination of

[9] Arvind Panagariya, *India in the 1980s and 1990s: A Triumph of Reforms*, IMF Working Paper No. 04/43, (Mar. 2004), https://www.imf.org/external/pubs/ft/wp/2004/wp0443.pdf.
[10] Manmohan Singh, *Budget Speech* for 1991-92, PARLIAMENT OF INDIA, (1991).

regulatory restrictions in phases, from a very restricted regime to one that overwhelmingly is in favour of the "automatic route" for most sectors, in which foreign investors could make investments without prior approval from the government, provided sectoral limits and other stipulations are respected.[11]

The primary framework for FDI in India is the Foreign Exchange Management Act, 1999 ("**FEMA**"), which replaced the previously more stringent Foreign Exchange Regulation Act, 1973 ("**FERA**").[12] FEMA, through various regulations and rules, most importantly the Foreign Exchange Management (Non-Debt Instruments) Rules, 2019 ("**NDI Rules**"), stipulates the modalities for foreign investment in India.[13] FDI can usually flow through the automatic route, allowing investment without advance clearance from the government, or the government approval route, required in specified sensitive sectors or in specified investment streams.[14]

A. THE MOVE TOWARDS STRINGENCY: THE BACKGROUND TO PRESS NOTE 3 (2020)

The policy environment was dramatically altered with the release of PN3 by the Department for Promotion of Industry and Internal Trade ("**DPIIT**") on April 17, 2020.[15] This act was mostly in answer to two related developments, which is the worldwide economic slowdown brought on by the COVID-19 pandemic, and the rising geopolitical tensions, specifically

---

[11] Panagariya, *supra* note 9.
[12] Foreign Exchange Management Act, 1999, No. 42, Acts of Parliament, 1999 (India).
[13] Foreign Exchange Management (Non-Debt Instruments) Rules, 2019, S.O. 3732(E) (Nov. 13, 2019) (India).
[14] *Id.,* Rule 16.
[15] *Supra* note 3.

between India's land border with China. The government sounded the alarm over "*opportunistic takeovers/acquisitions of Indian companies*" whose values took huge dives due to the pandemic, possibly by companies from land-borders.

PN3 was successful in modifying Paragraph 3.1.1 of the FDI Policy, which specified the government approval course of action.[16] Earlier the Para 3.1.1. reads "*A non-resident entity can invest in India, subject to the FDI Policy except in those sectors/activities which are prohibited. However, a citizen of Bangladesh or an entity incorporated in Bangladesh can invest only under the Government route. Further, a citizen of Pakistan or an entity incorporated in Pakistan can invest, only under the Government route, in sectors/activities other than defence, space, atomic energy and sectors/activities prohibited for foreign investment*." Under the revised position, it is Para 3.1.1(a) which reads "*A non-resident entity can invest in India, subject to the FDI Policy except in those sectors/activities which are prohibited. However, an entity of a country, which shares land border with India or where the beneficial owner of an investment into India is situated in or is a citizen of any such country, can invest only under the Government route. Further, a citizen of Pakistan or an entity incorporated in Pakistan can invest, only under the Government route, in sectors/activities other than defence, space, atomic energy and sectors/activities prohibited for foreign investment*"[17] and 3.1.1(b) which reads "*In the event of the transfer of ownership of any existing or future FDI in an entity in India, directly or indirectly, resulting in the beneficial*

[16] Press Note No. 3 (2020 Series) (DEP'T PROMOTION INDUS. & INTERNAL TRADE Apr. 17, 2020), https://cgishanghai.gov.in/pdf/PressNote3_23Nov2022.pdf.
[17] *Id* ¶1.

ownership falling within the restriction/purview of the para 3.1.1(a), such subsequent change in beneficial ownership will also require Government approval."[18]

After PN3, investment by an entity "*of a country, which shares a land border with India or where the beneficial owner of an investment into India is located in or is a citizen of any such country*" now mandatorily requires prior government clearance.[19] This is applicable both to indirect and direct investment and transfers of incumbent FDI. There are seven land-neighbouring countries of India, namely Bangladesh, Bhutan, China, Myanmar, Nepal, Pakistan, and Afghanistan.[20] Although the press note is seemingly country-neutrality-tilted in its choice of words, its timing and the larger political context made it unequivocally evident that China was the main target, considering its high investment footprint and the prevailing standoff along their land boundary.[21]

B. LEGAL IMPLICATIONS AND INSTANT EFFECT

The legal implication of PN3 is profound as it has effectively moved all investments, regardless of sector, originating from land-bordering countries, from the automatic route to the government approval route. This means that every such transaction must undergo a rigorous screening

---

[18] *Id* ¶2.

[19] *Supra* note 13.

[20] Rajat Sethi & Oshika Nayak, *Foreign Investment in India from Bordering Countries: A Case for Review*, CHAMBERS AND PARTNERS, (28 August, 2024), https://chambers.com/articles/foreign-investment-in-india-from-bordering-countries-a-case-for-review.

[21] ET Bureau, *Open to Rethink on Restrictions on FDI from China*, Says Official, ECONOMIC TIMES, Aug. 28, 2025, https://m.economictimes.com/news/economy/foreign-trade/open-to-rethink-on-fdi-from-china-import-restrictions-says-official-et-world-leaders-forum/articleshow/123551334.cms.

process by the Indian government, primarily through the Ministry of Finance, Department of Economic Affairs, or the concerned administrative ministry, depending on the sector.[22]

Responding instantly after its promulgation, PN3 received mixed reviews. For example, in context of procedural aspects, "*in April 2024, media reports quoting an anonymous source noted that out of a total 526 proposals received under PN3 since its introduction, 124 proposals were approved, and 201 proposals were rejected. The remaining 200 proposals remained pending, in some cases for several years.*"[23] While it was hailed by some as a much-required step toward safeguarding domestic industry and national assets, others, especially the investor community and lawyers, were alarmed by its possible chilling impact on FDI and the implementation difficulties of the PN3.[24] The confusion regarding essential definitions and procedures soon became evident and served as the prelude to the regulatory bottlenecks that are at the centre of this research. This change highlighted India's new national security paradigm, where economic sovereignty and strategic autonomy are increasingly being integrated with investment policy.[25]

---

[22] *Supra* note 13.

[23] *Sethi & Nayak, supra* note 20.

[24] Parina Mucchala, Prakhar Dua & Harshita Srivastava, *Foreign Investment in India from Neighboring Countries: Crossing the Chasm between Intent and Impact*, NISHITH DESAI ASSOCIATES (September 07, 2022), https://www.nishithdesai.com/fileadmin/user_upload/Html/Hotline/Regulatory_Digest_M_Sep0722.htm.

[25] Dep't of Econ. Aff., Gov't of India, *The Indian Economy – A Review (Jan, 2024)* https://dea.gov.in/sites/default/files/The%20Indian%20Economy%20-%20A%20Review_Jan%202024.pdf.

III. THE REGULATORY LABYRINTH: UNPACKING AMBIGUITIES IN PN3'S IMPLEMENTATION

In spite of its obvious purpose, the PN3 implementation has shown serious regulatory uncertainties that hamper its effectiveness and discourage investor confidence. They mostly concern the absence of a clear approval procedure, the vague shape of "*beneficial ownership*," and the mixed signals from AD banks.

A. THE OPAQUE APPROVAL FRAMEWORK AND LACK OF PREDICTABILITY

One of the major weaknesses of PN3's operationalization is the lack of clarity and predictability of the government approval procedure.[26] Unlike the previous Foreign Investment Promotion Board ("**FIPB**") regime, though controversial and reviled at times, the latter did evolve some sort of procedural parameters and timelines over time, PN3 fails to delineate clear SOPs for application processing.[27] Investors and lawyers are then routinely faced with a non-transparent procedure with very little understanding of the yardsticks used by the government for making approvals or rejecting applications, the decision-making matrix within the government, or clear timelines.[28]

---

[26] *Supra* note 17.

[27] Ananya Ahojoy and Param Kailash , "*Beneficial Owners, Borders and Bottlenecks: Evaluating India's FDI Policy under Press Note 3*" NUALS L.J, (Feb 9, 2025) https://nualslawjournal.com/2025/02/09/beneficial-owners-borders-and-bottlenecks-evaluating-indias-fdi-policy-under-press-note-3/.

[28] Shreya Gupta, *Foreign Direct Investment and Its Impact on India's Economic Growth*, 10 INNOVATIVE RESEARCH THOUGHTS 111 (2024).

This opacity gives rise to several challenges, such as the arbitrary discretion in which the failure to publish criteria for proposal appraisal vests substantial discretion with the government. Although national security arguments necessarily entail subjective judgment, the absence of objective yardsticks can provoke fears of arbitrary determination. It is not quite clear, for example, how the government delineates a "*sensitive*" investment deserving of scrutiny and a "*non-sensitive*" investment possibly capable of fast-tracking or exemption. Second, the extended timelines and transaction costs, where the absence of a clear processing time creates immense uncertainty and delay. Time-sensitive cross-border payments are not uncommon, and longer processing translates to increased transaction costs, additional market risks, and abandoned deals. Legal practitioners have registered applications stuck for months and sometimes more than a year, with no substantial updates or clear reasons for delay.[29] Additionally, the deterrence to investment in which predictability is a cornerstone of investor confidence. When the regulatory path is unclear and the outcome uncertain, foreign investors, especially those from land-bordering countries, are more likely to seek alternative destinations for their capital.[30] This "*chilling effect*" impacts not just the targeted countries but potentially India's overall appeal

[29] MINISTRY OF COMMERCE & INDUSTRY, *India offers a transparent, predictable and comprehensive FDI Policy Framework for investments*, (Feb. 11, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2101785.

[30] Authority to review certain mergers, acquisitions, and takeovers 50 U.S.C. § 4565 (2018), Foreign Acquisitions and Takeovers Act 1975 (Cth) (Austl.).

as an investment hub, as the general sentiment of stringency permeates the global investment community.

Comparative global practices show the need for investment screening transparency. The Committee on Foreign Investment in the United States ("**CFIUS**"), which is an interagency committee chaired by the Treasury Department, reviews foreign investments and real estate transactions for national security risks under Section 721 of the Defense Production Act. It uses a structured timeline, 30 days for initial review of notices, extendable to 45 days, with a 45-day investigation phase if risks are identified, allowing mitigation agreements or presidential blocks.[31] The Foreign Investment Review Board ("**FIRB**"), a non-statutory advisory body to Australia's Treasurer, assesses foreign investments under the Foreign Acquisitions and Takeovers Act using national interest and security tests. Applications face a 30-day initial review, extendable by up to 90 days via interim order, with mandatory notifications for national security actions and voluntary options for others. The Treasurer makes final decisions on approvals, rejections, or conditions, with public policy guidance fostering transparency.[32]

They have developed intricate regulatory processes, issued guidelines, and laid out timetables, allowing investors a better sense of the

---

[31] The Committee on Foreign Investment in the United States (CFIUS), U.S. DEPARTMENT OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

[32] Foreign Investment Review Board, FOREIGN INVESTMENT IN AUSTRALIA, https://foreigninvestment.gov.au/investing-in-australia/about-us/firb.

review procedure, even in national security-sensitive deals.[33] PN3 of India is not up to those global bests and hence erodes investor confidence about its regulatory predictability.

B. BENEFICIAL OWNERSHIP PUZZLE: CONCEPTUALIZING CONTROL OF CROSS-BORDER INVESTMENTS

Branch management can be put in a state of confusion about regulatory certainty under PN3, more than perhaps anything else, because of its very foundation on the term "*beneficial ownership*" and non-adoption of a clear, harmonized, and legally binding definition of it within the FDI policy architecture itself. PN3 clarifies that clearance is sought "*where the beneficial owner of an investment into India is located in or is a citizen of any such country*."[34] However, neither FEMA nor the NDI Rules, as amended by PN3, provides a clear definition of "*beneficial owner*" for this purpose.[35]

This definitional vacuum generates immense practical problems, such as inconsistencies in interpretations, in which, without a specific definition of their own, stakeholders end up using definitions from other Indian laws, which are quite diverse. For example, the Companies Act, 2013, refers to a "*significant beneficial owner*" as someone holding more than 25% of shares or votes or exercising significant control or influence.[36] Prevention of Money Laundering Act, 2002 ("**PMLA**"), and its rules

---

[33] *Supra* note 3.
[34] Mehta, *supra* note 4.
[35] Companies Act, 2013, § 90, No. 18, Acts of Parliament, 2013, (India).
[36] Prevention of Money-laundering (Maintenance of Records) Rules, 2005, G.S.R. 441(E) (July 1, 2005), as amended (India), at Rule 2(1)(g).

describe a beneficial owner as the person owning or controlling more than 25% of the shares or capital of a company or 15% of a partnership or exercising control through other mechanisms. SEBI laws may use other thresholds or yardsticks based on the context. This plurality of definitions results in inconsistent interpretations of PN3, with some using the threshold of 10%, others using 25%, and yet others taking a broader "*control*" view based on nothing but control.

There are identification issues in which it is always difficult to identify the "*ultimate beneficial owner*" ("**UBO**") of complex, multi-level corporate structures, particularly those that include intermediate holding companies, investment funds, or trusts. It is common for foreign investors to find it hard to follow the thread of ownership across multiple jurisdictions and impenetrable structures and hence to face dilemmas of compliance and higher due diligence costs. It is also confusing whether indirect ownership or influence alone is sufficient to bring PN3 requirements.

Moreover, there is a risk of non-compliance or over-compliance, in which the ambiguity places investors in a precarious position. A strict interpretation might lead to unnecessary applications for approval (over-compliance), delaying investments that pose no security threat. Conversely, a relaxed interpretation could risk non-compliance, attracting penalties under FEMA, including fines of up to three times the amount involved or

Rs. 100,000, and ongoing penalties.[37] This uncertainty breeds caution and can deter legitimate investments.

Not having a clear definition of beneficial ownership is not mere formalism; it has a direct impact on both the scope and efficiency of PN3 and makes it overreaching at times and evadable at others. International norms, such as those being promoted by the Financial Action Task Force ("**FATF**"), emphasize the need for accurate beneficial ownership disclosure in combating money laundering and terrorism financing and encourage India to align its definitions within regulatory regimes.[38]

C. THE AD BANK CONUNDRUM: CONFLICTING GUIDANCE AND OPERATIONAL HURDLES

AD banks are central to channelling FDI into India. They are the first-line regulators, responsible for processing inward remittances, ensuring that their transactions comply with FEMA, and reporting their transactions to the Reserve Bank of India ("**RBI**").[39] However, where PN3 is concerned, AD banks have given largely variable and occasionally conflicting advice to investors and corporate houses.

---

[37] Foreign Exchange Management Act, 1999, § 13, No. 42, Acts of Parliament, 1999, (India).

[38] Financial Action Task Force (FATF), *Guidance on Transparency and Beneficial Ownership*, (Mar 10, 2023) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Transparency-and-beneficial-ownership.html.

[39] Foreign Exchange Management Act, 1999, § 10, No. 42, Acts of Parliament, 1999, (India).

Their differences come in many forms, such as *first*, differing documentation requirements, in which AD banks require varying sets of documents from applicants, creating confusion and extra work of administration on the part of investors. Various banks may insist on very lengthy statements about ultimate beneficial ownership and corporate structures, and others may follow a more concise but possibly incomplete procedure.[40] *Second*, the pricing norms interpreted, where the FDI deals are regulated with certain pricing norms by FEMA so that valuation is fair and round-tripping or undervaluation is avoided.[41] Interpretations of pricing norms by AD banks in the light of PN3 requirement of government approvals, especially for transfers of shares or convertible securities, have been reportedly inconsistent and contributed to confusion about the monetary features of deals.[42] *Third*, there is a lack of clarity in the reporting procedure, in which the very details of what is required to be reported to the RBI under PN3 transactions, particularly the point at which government approval is sought and the point at which it is to be reported, have not been consistently interpreted by all the AD banks. This results either in finalization of the transaction being stuck or, more seriously, retrospective clarification sought by regulatory departments.[43]

---

[40] Praveenop, *supra* note 8.

[41] Foreign Exchange Management (Transfer or Issue of Security by a Person Resident Outside India) Regulations, 2017, G.S.R. 770(E), reg. 10 (Nov. 7, 2017), (India).

[42] Ashley Coutinho , *RBI Googly on Adherence to New Press Note 3 Norms Puts AIFs in a Bind*, BUSINESS STANDARD, (May 15, 2020), https://nishithdesai.com/Content/document/pdf/Quotes/200515_Q_RBI_googly_on_adherence_to_new_Press_Note_3.pdf.

[43] *Supra* note 17.

The absence of common circulars or holistic FAQs by the RBI specifically clarifying the role and responsibilities of AD banks under PN3, has aggravated this issue. Even though the RBI issues general instructions on FDI, the distinctive procedural features wrought by PN3 necessitate instructions specific to AD banks to achieve consistency and ease of implementation.[44] This operational bottleneck is yet another added complexity within a highly complex regulatory landscape and has spillover effects on the pace and predictability of capital flows.

IV. GEOPOLITICAL CROSSCURRENTS: FRAMING FDI POLICY IN A MULTIPOLAR WORLD

Indian PN3 adoption can only properly be appreciated within the larger framework of the new geopolitics underlying global investment flows. It is the confluence of rising protectionism, economic nationalisms, and strategic rivalries that has starkly redrawn the understandings of and regulation of foreign investment. For India, it is particularly the confluence of two larger geopolitical developments: its controversial relationship with China and its shifting strategic and commercial relationship with the United States.

[44] *Id.*

A. INDIA-CHINA INTERPLAY AND THE NATIONAL SECURITY URGENCY

The immediate and direct cause of PN3 was the ascending border tensions between India and China, particularly the recent 2020 military standoff in the Galwan Valley in June.[45] This development stoked long-standing suspicions regarding China's economic and strategic interests within India.[46] Anxiety was fanned by the perception that Chinese state-sponsorship enterprises would prey on India's economically fragile firms, amidst the context of the pandemic and utilize these strategic footholds to break into key industries.[47]

The national security compulsion by reason of India-China relations is multi-dimensional. *First*, the economic sovereignty in which there is growing concern about excessive dependence on China economically, especially in strategic sectors such as telecommunications, digital infrastructure, and supply chains of manufacturing. PN3 is regarded as a tool that can prevent China from acquiring controlling stakes or significant influence in entities that can contribute to China's strategic interests or gain access to sensitive information and technologies.[48] *Second*,

---

[45] *India-China Dispute: The Border Row Explained in 400 Words*, BBC NEWS (December 14 2022), https://www.bbc.com/news/world-asia-53062484 (last visited Sept. 1, 2025).
[46] Davide Donald, , *India Between Superpowers: Strategic Autonomy in the Shadow of a Pacific Conflict,* COUNCIL ON FOREIGN RELATIONS (Dec 16, 2024), https://www.cfr.org/blog/india-between-superpowers-strategic-autonomy-shadow-pacific-conflict.
[47] Amit Bhandari, Blaise Fernandes & Aashna Agarwal, *Chinese Investments in India,* GATEWAY HOUSE (Mar 9, 2020), https://www.gatewayhouse.in/chinese-investments-in-india/.
[48] Donald, *supra* note 46.

the worry about dual-use technologies, in which India and other nations are ever increasingly wary of foreign investment that can facilitate the export of dual-use technologies (technologies that can find both peacetime and wartime uses) to foes. High-technology manufacturing, artificial intelligence, and cybersecurity investment by foreign entities with Chinese government or People's Liberation Army ties is thus closely examined.[49] *Lastly*, the data privacy and security in which the data security has now become a fundamental part of national security due to the exponential growth of digital offerings. Data centre investment, e-commerce and digital payments made by Chinese companies are of concern due to possible data exfiltration, surveillance, or sabotages and hence the banning of some of the Chinese apps.[50]

Doctrinally, the justification of PN3 by the government is based on the right of a country to defend its national security and public order, a widely accepted principle of international trade and investment law.[51] But where the difficulty lies is delineating the line between proper national security concerns and generalized economic protectionism, where the investment is non-sensitive. The sweeping effect of PN3 encompasses all investments from land-boarding countries regardless of sector suggesting

---

[49] Dhruva Jaishankar & Tisyaketu Sirkar, *India's Tech Strategy: An Introductory Overview* — ORF AMERICA, (May 1, 2024), https://orfamerica.org/newresearch/india-technology-policy.

[50] Ministry of Electronics and Information Technology, Gov't of India, *Government Bans 59 Chinese Mobile Apps* (June 29, 2020).

[51] General Agreement on Tariffs and Trade 1994, Art. XXI (Security Exceptions).

where national security reasoning is extended stringently or nearly in blanket fashion.[52]

B. US-INDIA TRADE RELATIONS AND THE BROADER INTERNATIONAL INVESTMENT CLIMATE

Even though fundamentally oriented toward investment from neighbouring nations, PN3 implicitly informs India's overall trade and investment relations, particularly with its major partners like the United States. US-Indian relations, characterized by growing strategic convergence, economic connectivity, and cooperation on defence and technology issues, need an FDI policy aligned with the spirit of predictability and open markets but with protection for national security.[53]

PN3 has a nuanced impact on both US-India relations and the global investment climate. *First*, investment climate perception is there in which overall perception that the FDI policy of India is increasingly restrictive may discourage investment from non-target countries of PN3. Fears of regulatory unpredictability, although targeted at a limited group of countries only, may chill the investment prospects of all possible investing countries.[54] This is contrary to India's vision of luring foreign capital and being a manufacturing base, especially under programs like "*Make in India*." *Second*, is the compatibility with 'de-risking' trends in which the spirit of PN3, to cut dependence on potentially hostile supply chains and pre-screen

---

[52] *Supra* note 19.
[53] S. Jaishankar, *The India Way: Strategies for an Uncertain World*, at 167-175 (HARPER COLLINS INDIA 2020).
[54] Ahojoy & Kailash, *supra* note 27.

foreign investment based on their security risks, is congruent with the larger global trend of 'de-risking' or 'friend-shoring' supply chains, a policy that is increasingly being espoused by the US and other western economies.[55] India's approach, therefore, could find favour with those partners that are looking at resilient and secure supply chains. *Last*, is the attracting alternative investments by conveying a selective attitude toward investment from some geographies, India at the same time seeks to establish itself as a safe destination of capital from like-minded economies. But to do this fully, India needs to show a strong and clear regulatory framework of these alternative investments, which is undercut by the existing uncertainties of PN3 in non-sensitive sectors.

The geopolitical chessboard, therefore, poses a multifaceted difficulty faced by Indian policymakers such as protecting national security interests adequately without discouraging essential foreign capital from strategic allies and non-sensitive industries. PN3's existing framework of general application and inherent vagueness runs the risk of a suboptimal result by possibly over-controlling non-vital investments, and yet not being clear enough for effective security screening.

---

[55] Stefan Ellerbeck, *What Is 'Friendshoring'? This and Other Global Trade Buzzwords Explained,* WORLD ECONOMIC FORUM, Feb. 17, 2023, https://www.weforum.org/stories/2023/02/friendshoring-global-trade-buzzwords/.

V. BUILDING A CALIBRATED ROADMAP OF REGULATIONS: MERGING NATIONAL SECURITY AND INVESTMENT IN NON-SENSITIVE AREAS

The above discussion highlights the essential necessity of a calibrated PN3 approach that adequately protects India's national security interests while at the same time encouraging a favourable atmosphere of essential FDI into non-sensitive areas. A reform doctrinal roadmap involves a rectification of the identified fundamental ambiguities such as the opaque approval procedure, the unstated beneficial ownership, and the arbitrary AD bank procedure.

A. RESTRUCTURING THE APPROVAL SYSTEM: MAKING IT MORE TRANSPARENT AND PREDICTABLE

In order to achieve investor confidence and simplify the clearance system, India must head towards a predictable and clear regulatory system.

Proposition 1: Develop and Release Thoroughly Descriptive (SOPs) of PN3 Applications.

The government must place and promulgate standardized SOPs of processing PN3 applications, where the SOPs must detail with specificity about the specific criteria for assessment by detailed criteria that the government will consider when evaluating proposals, differentiating between sensitive and non-sensitive sectors. For instance, in non-sensitive sectors like basic manufacturing or non-critical technology, the assessment could focus primarily on economic benefit, employment generation, and competition rather than deep national security implications. Conversely,

sectors like defence, critical infrastructure, and advanced computing would warrant rigorous security vetting. Moreover, with clear timelines in which legally valid, reasonable, and prescribed timelines of acknowledgment, preliminary examination, detailed scrutiny, and final decision of the application processing at various stages. It can include a provision of 'deemed approval' in non-sensitive sectors in the event of not making a decision within a timeframe (90-120 days). Additionally, a designated nodal agency and inter-ministerial coordination in which even though a requirement of an inter-ministerial group is there, it is better if a central nodal agency (like DPIIT or DEA) is identified with a mandate of coordination and communication with applicants.[56] It is also required to carry out pre-application consultations so that the investors may get a sense of the requirements and probable scrutiny of the proposed investment.

Instituting the provision of clear, if brief, reasons for rejecting an application shall go a long way towards greater openness and shall help investors understand policy parameters and perhaps tailor-make future proposals.

Proposition 2: Introduce a Tiered Review System Based on Sector Sensitivity and Investment Value.

A 'one-size-fits-all' approach to investment screening is inefficient. Thus, a tiered system would allow for differentiated scrutiny. This can

[56] Off. of the U.N. High Comm'r for Hum. Rts., *Special Procedures of the Human Rights Council,* https://www.ohchr.org/en/special-procedures-human-rights-council/special-procedures-human-rights-council.

include an expedited review for non-sensitive sectors (e.g., textiles, certain FMCG, basic logistics, non-critical IT services, specific parts of manufacturing that do not involve dual-use technology), having a shorter timeline or even a simplified declaration regime, where full approval is only sought if specific security flags are triggered.[57] Additionally, an increased review of sensitive areas can maintain or raise the level of review of genuinely sensitive areas (i.e., defence, telecommunications infrastructure, strategic energy, space technology, next-generation semiconductors) as this is in line with global best practice where the vigour of screening is proportional to perceived risk.[58] Moreover, an investment value threshold of investment value, below which investment outside of sensitive sectors can fall within a yet more streamlined or automatic notification process, rather than full authorization. This would alleviate the administrative burden on the government side for smaller and less strategic investments.

B. DEFINITION OF "BENEFICIAL OWNERSHIP": COMMON DOCTRINAL APPROACH

The ambiguity surrounding "*beneficial ownership*" is a significant impediment. A clear, harmonized, and legally enshrined definition is essential for both compliance and effective screening.

---

[57] Dr. Martin Buntscheck *et al., Foreign Direct Investment Regimes Germany 2025*, INTERNATIONAL COMPARATIVE LEGAL GUIDES INTERNATIONAL BUSINESS REPORTS, (Nov. 15, 2024), https://iclg.com/practice-areas/foreign-direct-investment-regimes-laws-and-regulations/germany.

[58] The Committee on Foreign Investment in the United States (CFIUS), U.S. DEPARTMENT OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

Proposition 3: Take Up a Unified, Clear, and Threshold-Based Definition of "Beneficial Ownership" for FDI Applications.

The government should amend the NDI Rules or issue a unique circular or guidance note by DPIIT, after taking the views of the Ministry of Corporate Affairs and the RBI, and arrive at a common interpretation of "*beneficial owner*" to be used for PN3 purposes. It should define a clear ownership/control threshold, since the thresholds are diverse within Indian law; consistency is essential. A 25% or 10% threshold of ownership/voting rights, equivalent to the usual anti-money laundering requirements at the international level (e.g., FATF recommendations), can be used.[59] It is essential that the threshold defined is explicitly identified as the triggering point of PN3.

Also, approaching the indirect ownership and control as the definition has the requirement of expressly addressing how beneficial ownership is identified by indirect paths, e.g., by several layers of holding companies, trusts, or contractual arrangements that grant effective control. This is to include express provision for piercing corporate veils to discern the final natural person(s)[60].

Additionally, distinguishing between ownership and control provides a definition of "*control*" other than mere holding of shares that involves the right of selecting the majority of directors, right of exercising

---

[59] Financial Action Task Force, FATF Recommendations Rec. 10 & 24 (June 2021).
[60] Companies Act, 2013, No. 18, Acts of Parliament, 2013, § 90, read with Companies (Significant Beneficial Owners) Rules, 2018 (India).

influence on management decisions or other pervasive exercises of influence, with reference to the Companies Act, 2013.[61]

Proposition 4: Enforce Clear Declarations at All Levels of Ownership.

In addition to a clear definition, the government ought to enforce full disclosure requirements. It ought to require these investors to disclose all levels of ownership, up to the final natural persons that are the beneficial owners, with appropriate indemnity provisions for verification. This shall increase transparency and facilitate the government in its vetting process, making it more difficult to avoid the policy using intricate corporate structures.

C. STREAMLINING AD BANK PROTOCOLS: INCREASING CONSISTENCY

AD banks' role of frontline facilitator and regulator needs clear and unvarying advice.

Proposition 5: Clear and Consistent Circulars and FAQs Containing PN3 Implications Specifically for AD Banks Shall be Issued by RBI.

The Reserve Bank of India shall put out detailed and consolidated circulars and an exhaustive Frequently Asked Questions note after proper consultation with DPIIT and shall release these instructions to all AD banks. This clarification shall keep a standardized reporting forms in specifying standard reporting forms for PN3-related transactions so that data is submitted uniformly and regularly to the RBI. Moreover,

[61] Companies Act, 2013, § 2(27), No. 18, Acts of Parliament, 2013. (India).

simplification of clearing and documentation requirements where an exhaustive checklist of documents sought from investors for diverse PN3 deals so that discrepancies between banks are removed. Moreover, guidelines on pricing norms issues specific instructions on interpreting and applying FEMA pricing norms on PN3 transactions and on handling special valuation issues that may arise. At last, a centralized clarification mechanism provides a special desk or appropriate mechanism at the RBI where AD banks can go and seek clarifications on PN3-related issues so that interpretation is standardized throughout the banking sector.

Proposition 6: Regular Training and Sensitization of AD Bank Staff on PN3 Compliance.

The RBI and industry associations must mandate and regularly carry out training and sensitization of AD bank personnel responsible for FDI transactions. This advanced step will ensure that frontline staff are adequately aware and knowledgeable about the requirements of PN3, identification of beneficial ownership, and reporting mechanisms and hence reduce operational friction for investors.

With these presumptions, India is able to craft a mature regulatory framework that is robust when it comes to protecting national security but flexible enough to welcome and accommodate necessary foreign investment within its rapidly growing non-sensitive industries.

VI. CONCLUSION

India's PN3 represents a significant policy pivot, born out of legitimate national security concerns amplified by geopolitical tensions and the exigencies of the global pandemic.[62] Its intent to prevent opportunistic takeovers and safeguard strategic assets, particularly from land-bordering countries, is undeniably within the sovereign prerogatives of the Indian state. However, as this doctrinal analysis has demonstrated, the implementation of PN3, especially its broad application and the regulatory ambiguities embedded within its framework, risks undermining India's broader economic objectives by deterring crucial foreign direct investment, particularly in non-sensitive sectors.

This article reveals that, *first*, India can indeed relax the stringent requirements of PN3 in non-sensitive sectors without compromising its national security. The current blanket approach, which subjects all investments from land-bordering countries to the same rigorous and often opaque scrutiny, is disproportionate for sectors like basic manufacturing, non-critical technology, or certain services that pose minimal, if any, security risks. A calibrated, risk-based approach, distinguishing between genuinely sensitive and non-sensitive investments, is not only feasible but doctrinally sound, aligning India with global best practices in investment screening.

---

[62] Rajath Sethi & Deborshi Barat, *Geopolitical and National Security Considerations in Outbound Foreign Investment,* S&R ASSOCIATES, (Feb 13, 2024), https://www.snrlaw.in/geopolitical-and-national-security-considerations-in-outbound-foreign-investment/.

Second, the widespread regulatory uncertainties involving the approval framework and the meaning of "*beneficial ownership*" are remediable. The lack of transparency of the approval procedure, with features of non-publication of SOPs, uncertainties about timelines and express evaluation parameters, instills unpredictability and discourages investment. At the same time, the non-existence of a threshold-based, harmonized definition of "*beneficial ownership*" of FDI regulations results in varying interpretations, compliance costs, and risks of circumvention or over compliance. Elimination of these uncertainties by clear legislative changes or clarificatory authority is essential to install predictability and investor trust. *Lastly*, sectoral reforms of PN3 and AD bank-governing protocols are necessary to achieve the desired equilibrium between investor confidence and national interest. This article's roadmap suggests a multi-faceted approach, which involves improving the approval process' transparency and predictability with regard to detailed SOPs, tiered review mechanisms, and specified timelines; resolving the "*beneficial ownership*" puzzle with regard to a threshold-based, harmonized definition applicable throughout the FDI regime; and simplifying AD bank protocols with regard to detailed RBI circulars, uniform documentation format, and periodical training.

Successful management of this intersection, between protection of national security and openness to foreign investment, is central both to India sustaining its economic growth and pursuing the status of being a global economic leader. It will not only bring high-value FDI into non-sensitive areas but also reinforce India's status as a mature and predictable

investment destination. Further delay risks jeopardizing economic development and sending a signal of regulatory unpredictability, and thereby compromising both security and prosperity in the longer term.

Future work may investigate the empirical effect of PN3 on FDI inflows from certain land-bordering nations relative to other geographies, study the application success rates by sector, and carry out a more nuanced comparative study of other jurisdictions balance economic openness with national security interests. Such work would yield useful information to further calibrate India's FDI policy so that it remains dynamic, adaptive, and capable of serving both its economic growth and national security needs. Through it all, the ability of India to develop and clear a sophisticated regulatory architecture will determine its competitive advantage within a globalization movement toward yet increasingly fragmented investment climate.

Jagyansh Kumar & Sumit Patnaik, *The Domino Effect of Bank Failures: Do We Need a New Safe Harbour Insolvency Playbook?*, 12(1) NLUJ L. REV. 219 (2026)

THE DOMINO EFFECT OF BANK FAILURES: DO WE NEED A NEW SAFE HARBOUR INSOLVENCY PLAYBOOK?

~ Jagyansh Kumar & Sumit Patnaik[*]

ABSTRACT

*India's financial system is overwhelmingly bank-centric, which makes the failure of a major lender uniquely capable of triggering systemic disruption. Unlike ordinary corporate insolvencies, a bank failure affects thousands of counterparties simultaneously, NBFCs, corporates, mutual funds and clearing members forcing rapid repricing of risk and threatening economy-wide contagion. This article argues that India's current insolvency framework, which excludes banks from the IBC's Corporate Insolvency Resolution Process ("**CIRP**") and relies on ad hoc regulator-led interventions, lacks the predictability and calibrated sequencing needed to manage such events. The article suggests a sector-specific framework for India that combines enforceable safe-harbour safeguards with time-bound regulatory stays, drawing on comparative jurisprudence from the US and the EU, where safe-harbour regimes and bank-resolution instruments operate in tandem. It also accentuates how crucial bankruptcy-remote Special Purpose Vehicles ("**SPVs**") are for risk management and separating vital financial operations while the case is being resolved. This study illustrates how a coordinated, rule-based approach could compress risks, minimize contagion, and protect systemic stability in a bank-dominated*

[*] Jagyansh Kumar and Sumit Patnaik are third-year students at National Law Institute University, Bhopal.

credit economy by analysing seminal cases like Dharani Sugars v. Union of India and the Yes Bank disaster.

TABLE OF CONTENTS

I. INTRODUCTION 222

II. DEMYSTIFYING SAFE HARBOURS FOR BANKING INSOLVENCY 226

A. SAFE HARBOURS: FINANCIAL CONTRACTS AND INSOLVENCY 226

B. COMPARATIVE NOTE ON THE USA AND THE EU'S EXPERIENCE WITH SAFE HARBOURS 230

I. USA'S QUALIFIED FINANCIAL CONTRACTS 230

II. EU'S FINANCIAL COLLATERAL DIRECTIVE AND BRRD 231

III. INDIA'S CURRENT LEGAL POSITION REGARDING EXCLUSION OF BANKS FROM THE IBC 233

A. THE CRISIS OF PMC BANK 234

B. THE YES BANK CRISIS 237

IV. JUDICIAL VIEWPOINT IN INDIA: DHARNI SUGARS IN REFERENCE 238

V. EMBEDDING NETTING CERTAINTY AND CALIBRATED SUSPENSION IN INDIA'S BANK-RESOLUTION STATUTE 243

VI. CONCLUSION 248

I. INTRODUCTION

India's financial system remains deeply reliant on the banking sector to act as a credit intermediation channel between companies. Generally, when companies come under the Corporate Insolvency Resolution Process ("**CIRP**"), secured creditors, which generally include banks, have a priority interest in the Committee of Creditors ("**CoC**").[1] The Insolvency and Bankruptcy Code of India ("**IBC**") broadly applies to corporate structures, limited liability companies, individuals, partnerships and other entities.[2] However, the statute explicitly excludes financial service providers ("**FSPs**"), including banks, from its definition of corporate debtor under Section 3(17) of the IBC.[3] The National Company Law Appellate Tribunal ("**NCLAT**") has reaffirmed this position that FSPs fall outside the ambit of the CIRP under the IBC.[4] Consequently, banks are not hit by IBC's creditor-in-possession CIRP model, and importantly, remain outside the ambit of moratoriums.[5] Banks are regulated under the Banking Regulation Act, 1949, which confers power on the Reserve Bank of India ("**RBI**") to initiate restructuring plans of banks, as seen in numerous cases.[6] The exclusion is not an oversight, for there is an important policy choice. Unlike ordinary corporate debtors, such as companies, banks are engaged in critical financial functions such as deposit taking, payment settlement, flow of

---

[1] Committee of Creditors of Essar Steel India Ltd. v. Satish Kumar Gupta & Ors., (2019) 2 SCC 1.
[2] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 2 (India).
[3] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 3(17) (India).
[4] Globe Capital Market Ltd. v. Narayan Securities Ltd., 2024 SCC OnLine NCLAT 122.
[5] Siksha Bansal, *NBFCs and IBC: The Lost Connection*, BAR AND BENCH (Oct. 11, 2018) https://www.barandbench.com/columns/nbfcs-and-ibc-the-lost-connection.
[6] Banking Regulation Act, 1949, No. 10 of 1949, § 45 (India).

money in the economy, etc. Henceforth, a blanket moratorium can jeopardize the wider financial system. However, it also leaves India in a limbo of a predictable, rule-based mechanism for resolving bank failures, which raises an important question: whether the current Indian insolvency framework is sufficiently equipped to deal with bank failures in a way that preserves systemic stability.

India's credit intermediation is overwhelmingly bank-centric, and a failure at a large lender can rapidly set off funding freezes, collateral fire sales, and payment gridlock that spread to borrowers and their suppliers.[7] That ripple effect is the starting point of this article. Ordinary corporate insolvency tools under the IBC are too slow and too symmetry-oriented for a node as interconnected as a bank. Unlike an ordinary corporate debtor, the failure of a bank disrupts not only its creditors but also thousands of counterparties, including cash-rich corporates, NBFCs, mutual funds, and clearing members who are forced to reprice risk simultaneously.[8] In such a scenario, a liquidity shock can swiftly mutate into an economy-wide solvency crisis. This creates a more nuanced policy question than the one asked in the preceding paragraph: whether India's present toolkit adequately distinguishes between the failure of a bank, a systemic utility, and the failure of an ordinary company and, if not, whether targeted 'safe harbours' should be extended to the banking context to contain contagion. Safe harbours are narrowly tailored statutory walls that insulate certain

[7] Ramprasad Verma et al., *Analysing the systemic risk of Indian banks*, 176 ECONOMIC LETTERS 103, 105.
[8] *Id.*

financial contracts, such as derivatives, repurchase agreements ("**repos**"), and netting arrangements, from consequences of insolvency, such as a moratorium. They prevent the implications of freezing time-sensitive market transactions that could jeopardise the financial system. A detailed account of such statutory walls is done in Part II of this article. In this context, it is important to refer to a shelved, dedicated bank-resolution statute, the Financial Resolution and Deposit Insurance Bill, 2017 ("**FRDI Bill**"), which was withdrawn in 2018 over bail-in concerns and has not been enacted with a replacement.[9] Considering this, it is imperative to refer to foreign legislation on the subject matter that has tackled the issue to break contagion chains from bank failure to the wider economy and to keep payment, deposit, and credit functions running. This aspect will be dealt with in detail later in this article.

When a bank fails, the challenge for policymakers is to stabilise the system without paralyzing counterparties that rely on timely settlement and liquidity. Ordinary insolvency tools accentuate creditor equality and procedural symmetry, but in the case of banks, with dense interconnectedness, such symmetry can amplify, rather than contain, contagion. This has led many jurisdictions to design specialised safe harbours within their resolution regimes. For instance, the European Union ("**EU**") preserves close-out netting, and collateral enforcements under the Financial Collateral Directive ("**FCD**"), while simultaneously empowering resolution authorities under the Bank Recovery and Resolution Directive

[9] Press Information Bureau, *Clarification on FRDI Bill*, MINISTRY OF FINANCE (Jul. 27, 2020) https://www.pib.gov.in/PressReleasePage.aspx?PRID=1641568.

("**BRRD**") to impose a narrowly time-bound stay to facilitate proper resolution.[10] The rationale is not to privilege specific creditors *per se*, but to prevent system-wide disruption when thousands of contracts are suddenly frozen.[11] India, however, has only taken partial steps in this direction. The Netting Act provides certainty in the enforceability of bilateral netting arrangements, but it does so in isolation, outside of a broader bank-resolution framework.[12] What is missing is a coherent playbook that coordinates temporary regulatory stays with such protections, in the manner of the other legislations.

With this legal and comparative foundation, the animating hypothesis is simple: a narrowly tailored, sector-specific safe-harbour architecture integrated into a modern bank-resolution code can greatly reduce insolvency contagion from banks to the corporate economy without sacrificing fairness or discipline. Accordingly, the article proceeds in four moves, with this being Part I. Part II first builds the safe-harbour concept from contract up: master agreements, close-out netting and why these protections are systemically valuable. Part III then maps India's current position in the IBC regarding the exclusion of banks and the selective use of Section 227 for FSPs, with a few notable cases. Next, Part IV evaluates

---

[10] Directive 2002/47/EC, art. 7, of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, 2002 O.J. (L 168) 43.

[11] Philip Paech, *The Value of Insolvency Safe Harbours,* LSE Law, 9/2015 SOCIETY AND ECONOMY WORKING PAPERS, 3.

[12] Bhavya Gupta, *Analysis of the Bilateral Netting of Qualified Financial Contracts Act, 2020*, SCC ONLINE (Feb. 6, 2021) https://www.scconline.com/blog/post/2021/02/06/analysis-of-the-bilateral-netting-of-qualified-financial-contracts-act-2020.

whether and how those protections should be embedded in a bank-resolution statute, calibrating limited regulatory stays with the Netting Act to avoid value-destroying gridlock. Part V turns to jurisprudence evolved by the courts in this subject matter to show how Indian courts have already grappled with systemic-risk logic in adjacent contexts and to extract design lessons for a bank-specific framework. Lastly, Part VI explores bankruptcy-remote structures as complements, not substitutes, to resolution and safe harbours, clarifying when asset segregation reduces contagion and when it merely shifts losses. The article will conclude by offering policy suggestions on the issue of regulating banking insolvency in the context of such methods and posit a positive way forward.

II. DEMYSTIFYING SAFE HARBOURS FOR BANKING INSOLVENCY

A. SAFE HARBOURS: FINANCIAL CONTRACTS AND INSOLVENCY

Safe harbours, originally, are concepts, or rather, exceptions applied in financial contracts.[13] Such arrangements have been dealt with under the US Bankruptcy Law, where the doctrine is applied to certain financial contracts, such as securities contracts, commodity contracts, forward contracts, repos, swaps and other derivatives, and master netting agreements.[14] The main purpose of creating such an exception is to protect the non-liquidating party from the risk of losing its assets during the insolvency process of the liquidating party. Since financial contracts

[13] Paech, *supra* note 11.

[14] Charles W. Mooney Jr., *The Bankruptcy Code's Safe Harbors for Settlement Payments and Securities Contracts: When Is Safe Too Safe?* 49 TEXAS INT'L LAW JL 243, 244 (2014).

introduce new challenges to the standard insolvency process, the safe harbour doctrine offers a way to manage these complex mechanisms. The doctrine protects parties from general principles of insolvency law, such as the *pari passu* principle, moratorium, creditor claims, etc.[15] Typically, insolvency law frameworks are designed to safeguard the assets of the debtor and to ensure that the company continues as a 'going concern'. This can vary significantly across different jurisdictions, as India provides a debtor-friendly framework, whereas the UK and EU adopt a more creditor-centric approach to insolvency matters.[16] Nevertheless, the implementation of such an approach remains likewise for every stakeholder in the transaction. This treatment, although necessary, creates crashing implications for financial contracts, and by extension, creates a domino effect on the banking sector. To understand the above exposition, a brief perusal of the mechanics of banking setups is pertinent. Unlike ordinary corporations, financial institutions serve as critical nodes in an intricate, woven web of obligations. The most commonly employed nodes are banks. Therefore, a failure of such an institution is not limited to the contracting parties, as banks acting as creditor nodes to several such contracts amplify the insolvency risk of other companies and disrupt liquidity flows in the economy. This is the point where safe harbour provisions come in. As stated earlier, acting as statutory insulators against insolvency

---

[15] Paech, *supra* note 11.

[16] Sparsha Pavan & Sidharth S, *Shift in Control – Debtor in Possession to Creditor in Control,* IBC LAWS (Feb. 28, 2024) https://ibclaw.in/shift-in-paradigm-debtor-in-possession-to-creditor-in-control-by-adv-sparsha-pavan-ca-sidharth-s/; VANESSA FINCH, CORPORATE INSOLVENCY LAW: PERSPECTIVES AND PRINCIPLES, 28-35 (2nd ed. 2009).

consequences, they permit the non-defaulting parties to terminate contracts, enforce collaterals attached to their arrangements, and close out net positions notwithstanding the debtor's insolvency. This ultimately tackles the 'contagion risk', the critical issue in banking insolvency. However, this equal treatment of companies and banks alike can become a source of contagion in financial markets.[17]

A useful way to understand this contagion risk is by looking at repurchase agreements. A repo is essentially a short-term loan where one party sells securities to another party with a promise to buy them back at a slightly higher price after a short period.[18] If repos were treated under ordinary insolvency rules, without safe harbours, the lender who supplied cash through a repo would be forced to wait in line with other creditors during insolvency proceedings as per the *pari passu* principle, unable to immediately sell the collateral securities. This delay is disastrous because repo lending is time-sensitive and depends on the lender's ability to liquidate collateral instantly if the borrower defaults. If that right is suspended, lenders lose confidence and pull back from the market. The immediate result is a freeze in short-term funding, and the shock quickly spreads: other institutions that depend on repo funding find themselves unable to roll over their obligations, leading to fire sales of assets, plummeting prices and further defaults. This chain reaction is the essence of contagion. The failure of one institution cascades through the financial

---

[17] Stephen J. Lubben, *Derivatives and Bankruptcy: The Flawed Case for Special Treatment* 12 U. PA. J. BUS. L. 61, 64 (2009).

[18] Jeffrey Cheng & David Wessel, *What is the repo market, and why does it matter?* BROOKINGS (Jan. 28, 2024) https://www.brookings.edu/articles/what-is-the-repo-market-and-why-does-it-matter.

system, not because of direct losses alone but because confidence and liquidity evaporate at the same time. Safe harbours break this cycle by allowing repo counterparties to enforce collateral and close out positions instantly, compressing exposures before they spiral out of control.

Several notable examples exist for this phenomenon. The collapse of Bankhaus Herstatt in 1974 remains one of the earliest and most influential instances.[19] When German regulators withdrew the bank's license at the end of the business day in Frankfurt, counterparties who had already delivered Deutsche Marks in settlement were left without their dollar payments from New York. This mismatch in settlement cycles triggered severe disruption across the global foreign exchange markets and gave rise to what is now termed 'Herstatt risk'.[20] A more recent and equally illustrative example is the bankruptcy of Lehman Brothers Holdings in 2008.[21] With nearly 900,000 derivative positions open at the time of its filing, Lehman's entry into Chapter 11 proceedings precipitated an unprecedented unwinding of financial contracts. The simultaneous termination of derivatives agreements by counterparties, combined with uncertainties about collateral enforcement across multiple jurisdictions, created a liquidity freeze and aggravated the global financial crisis.[22] The

---

[19] *Herstatt Risk: Lessons from the Collapse of Bankhaus Herstatt*, SLM MBA (Mar. 8, 2024) https://slm.mba/mmpb-004/herstatt-risk-collapse-bankhaus-herstatt.
[20] *Id.*
[21] Yassine Bakkar, *Why did Lehman Brothers fail?* ECONOMICS OBSERVATORY (Sept. 28, 2023) https://www.economicsobservatory.com/why-did-lehman-brothers-fail.
[22] Stephen J. Lubben, *The Bankruptcy of Lehman Brothers: An Empirical Study*, 22 AM. BANKR. INST. L. REV. 141, 145-49 (2014).

inability of general insolvency law to account for the interconnectedness of Lehman's exposures demonstrated, in stark terms, the inadequacy of conventional insolvency principles when applied to systemically important financial institutions.

B. COMPARATIVE NOTE ON THE USA AND THE EU'S EXPERIENCE WITH SAFE HARBOURS

i. USA's Qualified Financial Contracts

One of the most developed notions of safe harbours under insolvency regimes exists in the US, where the US Bankruptcy Code itself extends special treatment to certain Qualified Financial Contracts ("**QFCs**") such as securities contracts, repos, swaps, and other derivatives. "Qualified financial contract" means a bilateral financial agreement that a competent authority designates as a QFC and typically comprises securities contracts, commodity contracts, forward contracts, repurchase agreements, swaps, securities lending and similar OTC derivative and margining arrangements. The label exists to secure enforceable bilateral netting, close-out, and priority rules in insolvency or resolution. The precise scope and the regulators empowered to notify QFCs vary by jurisdiction.[23] The Code seeks to exempt such contracts from the automatic stay of moratoriums,[24] the prohibition on *ipso facto* clauses,[25] and certain trustee avoidance powers.[26] In effect, they allow non-defaulting counterparties to terminate, net and realise collateral immediately upon the insolvency of a counterparty. In the

[23] Bilateral Netting of Qualified Financial Contracts Act, 2020, § 2(n) (India).
[24] 11 U.S.C. § 362(b)(6)-(7), (17), (27) (2018).
[25] 11 U.S.C. § 365(e)(1), 541(c)(1) (2018).
[26] 11 U.S.C. § 546(e)-(g), 546(j) (2018).

netting process, only the net amount, which is the total owed by the parties after calculation, is to be returned by the party with the surplus debt.[27] Such carve-outs are intended to prevent the default of a single institution from cascading through financial markets by ensuring that firms can handle the contagion effect and recover collateral without delay. Therefore, both counterparty credit risk and systemic contagion are reduced, as a failing institution's default is contained rather than transmitted through chains of unsettled trades.

ii. EU's Financial Collateral Directive and BRRD

The EU's approach to this provision is more layered. The EU has enacted two main legislations to legislatively recognise such exceptions, namely the Financial Collateral Directive ("**FCD**") and the Bank Recovery and Resolution Directive ("**BRRD**"). Under the FCD, Article 7 provides for close-out netting and collateral arrangements to be legally enforceable, which allows counterparties to reduce their exposures to a failing institution by offsetting obligations and actualising pledged collateral.[28]

The BRRD acts as complementary or perhaps overlapping legislation, with a more systemic dimension by granting resolution authorities specific powers to intervene in the failure of a bank. Article 71 of the BRRD grants resolution authorities the power to impose a temporary

---

[27] Stephen Adams, *Derivatives Safe Harbours in Bankruptcy and Dodd-Frank: A Structural Analysis,* HARVARD LIBRARY (April 30, 2013) https://dash.harvard.edu/server/api/core/bitstreams/7312037c-f79a00-6bd4-e053-0100007fdf3b/content.

[28] Directive 2002/47/EC, art. 7, of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, 2002 O.J. (L 168) 43.

suspension of termination rights generally limited to 24 or 48 hours under Article 71(2),[29] with the objective of enabling the implementation of a resolution plan. Such a plan may include the transfer of assets and contracts to a bridge institution or a purchase and assumption transaction with a private-sector purchaser.

Together the FCD and BRRD create a dual mechanism where, on the one hand, counterparties retain legal certainty that their netting and collateral rights will be preserved under the FCD. On the other hand, resolution authorities are given a narrow but crucial window to coordinate an orderly resolution and prevent destabilising cascades of contract terminations. These provisions have been tailored to these foreign legislations. However, what remains to be seen is how India approaches this exception. The Bilateral Netting of Qualified Financial Contracts Act, 2020 recognises close-out netting arrangements in isolation, but without an integrated bank resolution framework akin to the BRRD. In this regard, the current position of banking insolvency in India is dealt with in detail in the next section, where the author shall examine the statutory exclusion of banks from the IBC and the regulatory mechanisms that presently govern bank distress.

[29] Directive 2002/47/EC, art. 71, of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, 2002 O.J. (L 168) 43.

III. INDIA'S CURRENT LEGAL POSITION REGARDING EXCLUSION OF BANKS FROM THE IBC

In the current legal scenario, banks are excluded from the purview of the IBC under Section 3(7),[30] which expressly excludes Financial Service Providers ("**FSPs**") from the statutory notion of corporate debtor. According to Section 3(17), a financial services provider is someone who is authorised or registered by a 'financial sector regulator' to offer financial services. As per the statutory meaning, services such as NBFCs, microfinance institutions, etc. would be qualified to be called FSPs and not banks. Thereby, banking, which provides maturity and liquidity transformation, intermediate repos, participates in payment and settlement systems, and carries contingent exposures through derivatives, is governed by the Banking Regulation Act, 1949. An alternate reason would be that banks do not function as regular financial providers and are deeply interconnected with the financial system of an economy, and considering the systemic consequences that any economy will go through should regular insolvency proceedings be imposed on a bank, the legislature developed a different law for the banking sector, although the law remains at a nascent stage.

India's recent experience demonstrates the consequences of relying on non-statutory, ad hoc measures when a bank becomes insolvent. In this article, we discuss two important episodes: the Punjab & Maharashtra Co-

[30] Insolvency and Bankruptcy Code, 2016, No. 31, Acts of Parliament, 2016, § 3(7) (India).

operative ("**PMC**") Bank crisis and the Yes Bank crisis, which expose the limits of the nascent legislation and underscore the social and economic costs borne by depositors and debtors when recovery is managed on an ad hoc basis.

The first step for the bailout of such banks by the RBI is to increase the capital of the banks, but this is not realistically possible if those transactions that benefit the bank are also blocked due to the moratorium. Practically speaking, a moratorium that freezes payments and receipts cripples the bank's transactional engine, which ultimately interrupts the flow of funds necessary for normal intermediation and, crucially, hinders recapitalisation efforts. Sources of fresh capital and liquidity coming from private investors, market-based financing, or even regulatory recapitalisation plans are harder to realise when the institution's business is functionally paralysed. RBI exercised its regulatory powers, superseding the bank's board and assuming control, a reactive intervention that highlighted the absence of a predefined statutory resolution path set out for banks.

Let us delve deeper into this by looking at two large scale episodes affecting the banking structure of the Indian economy.

A. THE CRISIS OF PMC BANK[31]

The PMC Bank crisis unfolded publicly in late September, 2019 after the RBI invoked its powers under the Banking Regulation Act, 1949 and imposed a supervisory restriction on core banking operations. The

[31] Shakeel, M. R., Siddiqui, T. A., & Siddiqui, S., *PMC Bank Debacle: A Failed Corporate Governance Case*, 7(2) EMERGING ECONOMIES CASES JOURNAL, 62-66 (2024) https://doi.org/10.1177/25166042241274843.

restriction, communicated on 24 September, 2019, effectively suspended loan renewals and issuances, prevented acceptance of fresh deposits, and halted most payments while permitting only limited disbursements for salaries and essential office expenses. The moratorium was accompanied by an operational freeze. ATMs and online services were withdrawn, and daily withdrawal limits were imposed on all depositors, the frequently cited cap being INR 1,000 per account. These measures stopped an immediate run but also immobilised the bank's normal intermediation functions and its ability to receive rescue capital.

Subsequent inquiries revealed that the bank's exposure to the HDIL group was vast and materially understated. The actual net exposure to the HDIL group was approximately INR 62.26 billion, representing roughly three quarters of the bank's loan book, whereas PMC's regulatory filings reported only a small fraction of this exposure. The mismatch between the reported Non-Performing Assets ("**NPA**") and the bank's real asset quality was achieved through an elaborate scheme of misreporting and the use of fictitious or surrogate accounts. Investigators identified over 21,000 such phony accounts used to mask the HDIL group's borrowings. The concentration of related party lending, the concealment of defaults, and the failure of auditors to flag these differences collectively transformed a solvency problem into a sudden crisis that affected depositors' access to funds.

The imposition of withdrawal restrictions during the festive season had immediate human consequences. Media reports and enquiries recorded

instances of severe distress among depositors who could not meet committed payments or medical expenses, there were multiple reports of depositors dying after being unable to obtain necessary funds.[32] The crisis also resulted in legal and regulatory action, criminal arrests, suspension of office-bearers, prosecutions of auditors, and the initiation of investigations by the Economic Offences Wing and the Enforcement Directorate, which later attached properties worth several thousand crores.

Now, consider an ordinary depositor who has placed life savings in an account to meet a committed expense, for example, a house purchase that is due within a month, and who finds that withdrawals are capped at a nominal sum per day. Such measures, though perhaps necessary to stem a run, impose severe hardship on individual households. This showcases that the insolvency of banks should not be equated to a simple insolvency proceeding against a corporate debtor due to the systemic consequences that follow. India's well-known cooperative bank failed miserably, and the whole country was in for an economic shock.

The episode exposed two related gaps. *First*, India lacked a predictable, legislated resolution pathway tailored to banking failures. The Banking Regulation Act, 1949 amendments that followed, which were introduced by the Hon'ble Finance Minister, strengthened supervisory powers but did not, on their own, create a calibrated aftermath process that preserves an operating bank's capacity to receive capital during a supervisory freeze. *Second*, existing safeguards for small depositors, who

[32] Nidhi Rai, *PMC Bank collapse: "We lost our money and then our son"*, BBC NEWS (Sept. 25, 2020), https://www.bbc.com/news/world-asia-india-54261121.

face hardship when daily withdrawal caps are imposed, proved inadequate. The insurance and payout mechanisms were also slow and cumbersome.

This leads us to another similar episode where the effects were even more evident and on a much larger scale, which trembled the Indian economy and forced it to reconsider the banking and insolvency structure.

B. THE YES BANK CRISIS

The Yes Bank crisis was another major crisis in the Indian banking industry, which shook the Indian populace. The bank was susceptible to giving away bad loans, which ultimately led to its downfall. RBI took control of its operations and issued a 30-day moratorium, which resulted in all types of transactions being blocked.[33]

The loan amount of Yes Bank was surpassing around Rs. 40,000 crores (Gross NPA). Furthermore, they were continuously giving out huge loans to big firms and companies such as Essel Group, Reliance etc. This led to deterioration in asset quality, rising non-performing exposures, and a concomitant loss of depositors. This, along with a loss in market confidence, triggered a liquidity squeeze, ultimately resulting in the failure of the bank's operations. In line with a policy of preserving financial stability, the government determined that Yes Bank should be rescued and therefore directed the State Bank of India to acquire a 49% stake in order to stave off bankruptcy. This method of insolvent proceedings is not explicitly mentioned in any legislation. Hence, the proceedings of such

[33] Srivastava, Anvesha & Rai, Prakhar, *From Trust to Turmoil - The Yes Bank Financial Scam*, IFSA NETWORK (Mar. 9, 2025).

situations are always chaotic due to a lack of an established procedure. An established statutory regime comparable to the US, differentiating categories of bankruptcy and prescribing procedures for each, creates a clear and predictable mechanism for resolving insolvency matters. Then the government wouldn't have to take such drastic measures, and there wouldn't be any domino effect, which would risk a collapse of the economy.

In order to fill this legislative gap, India requires a clear, statutory bank-resolution framework along with the indoctrination of safe harbour doctrines. As we have already seen, the ordinary CIRP provisions were never intended for banks or FSPs. This means that due to a lack of such specified legislation, regulators have had to invoke Section 35AA of the Banking Regulation Act, 1949,[34] to supersede boards and Section 45 to impose a moratorium,[35] thus producing reactive case-by-case fixes rather than a predictable statutory process. This results in depositor uncertainty, such as withdrawal caps, phased access, and reputational risk for the system, which a definite resolution plan can easily mitigate.

IV. JUDICIAL VIEWPOINT IN INDIA: DHARNI SUGARS IN REFERENCE

From our discussions in the preceding sections, the theoretical understanding of the safe harbours under the insolvency regimes of different countries has been laid down. As Part II clearly highlighted the need for such special exceptions to be carved out to mitigate the risks of an

[34] Banking Regulation Act, 1949, No. 10 of 1949, § 35AA (India).
[35] Banking Regulation Act, 1949, No. 10 of 1949, § 45 (India).

insolvency contagion in the banking sector, this section will particularly focus on the nascent judicial development of such banking insolvency contagion in India. The crisis of Yes Bank and PMC Bank also accentuates the need for evaluating the judiciary's position on the issue to incorporate this exception in the banking insolvency framework. The focus of this heading will be on the Supreme Court's stance in *Dharani Sugar v. Union of India.*[36]

Before delving into the merits of the judgment, a brief background of the events leading up to this case is pertinent to discuss. The IBC recently came, providing a completely new framework for revitalisation of the stressed assets, which placed mounting levels of pressure on the banking system to develop compliance procedures with the legislation. The Banking Regulation (Amendment) Ordinance, 2017, promulgated on 4 May, 2017, inserted Sections 35AA and 35AB into the Banking Regulation Act, 1949, empowering the Central Government to authorise the RBI to direct banks to initiate insolvency proceedings under the IBC and permitting the RBI to issue directions for the resolution of stressed assets. Pursuant to this empowerment, the Ministry of Finance issued an order dated 5 May, 2017 authorising the RBI to exercise such powers.[37] Subsequently, the RBI issued its 'Resolution of Stressed Assets – Revised Framework' circular on 12 February, 2018, consolidating prior schemes such as CDR, SDR, and S4A,[38] and mandating that, for accounts with aggregate exposure of INR 2,000

[36] Dharani Sugar v. Union of India, AIR 2019 SC 305.
[37] *Id.* ¶4.
[38] *Id.* ¶13.

crore or more, insolvency proceedings be initiated under Section 7 of the IBC within 15 days of the expiry of 180 days from default if no resolution plan was implemented. This circular became the primary subject of challenge, with petitioners arguing that the RBI had acted beyond its statutory authority under Section 35AA and that the circular disproportionately impacted sectors such as power, sugar, and shipping.

The principal question was whether the RBI's circular dated 12 February, 2018 was *ultra vires* Section 35AA of the Banking Regulation Act, 1949, specifically, whether RBI could direct banks to initiate insolvency proceedings in respect of a class of debtors absent a case-specific authorisation by the Central Government. The circular effectively functioned as a 'super trigger', compelling simultaneous insolvency filings across multiple large borrowers, which, if left unchecked, could have contagion effects, the central theme of this article.

The petitioners, representing power producers, sugar mills, shipping companies and other stressed sectors, contended that the 12 February, 2018 circular was *ultra vires* Section 35AA of the Banking Regulation Act. They argued that Section 35AA permits the RBI to direct initiation of insolvency only 'in respect of a specific default' and 'by such bank or banks,' pursuant to an express authorisation from the Central Government.[39] A blanket direction covering all accounts with exposures above INR 2,000 crore, they submitted, failed this specificity test. The petitioners further argued that the circular violated the principle of proportionality and Article 19(1)(g) of the Constitution, as it imposed a one-

[39] *Id.* ¶18.

size-fits-all approach on sectors such as power, which suffered from systemic issues beyond the control of borrowers, for instance, fuel shortages and discom payment delays. They highlighted the risk of pushing otherwise viable units into insolvency, potentially triggering massive haircuts for banks and asset value destruction. The petitioners also raised that the same question of law was dealt with by the Allahabad High Court in *Independent Power Producers Association of India v. Union of India and Ors*.[40]

The Union of India and the RBI, on the other hand, defended the circular as a necessary measure to deal with mounting NPAs and argued that Section 35AA, read with 35AB, conferred sufficient power on the RBI to issue directions for class-wide resolution of stressed assets. They argued that giving banks discretion would perpetuate 'evergreening' of loans and delay resolution, thereby worsening the NPA crisis. The RBI also stressed that the circular was prospective and gave banks 180 days to implement resolution plans before mandating IBC reference. While dealing with these issues, the Supreme Court engaged in a close textual reading of Section 35AA and contrasted it with Section 35A, which provided for the RBI's general power to issue directions in public interest. Justice Rohinton F. Nariman, writing for the Bench, ruled that Section 35AA was a specific provision carved out to deal with defaults leading to IBC referrals and that its language contemplated directions '*in respect of a specific default by a specific debtor*', effectively a measure *in personam* rather than *in rem*. The Court held

[40] Independent Power Producers Association of India v. Union of India and Ors., 2018 SCC OnLine All 4611.

that Parliament's choice of words reflected its intent that the extraordinary step of pushing a borrower into IBC should be exercised only on a case-by-case basis. The 12 February, 2018 circular, however, operated at a class level, it covered all accounts above INR 2,000 crore that were in default on a given date, without any individualised application of mind or specific government authorisation for each case. This, the Court concluded, transgressed Section 35AA's limits and was therefore *ultra vires*. The Court's reasoning rested heavily on legislative intent: Section 35AA was introduced by the 2017 Amendment to provide a narrowly tailored mechanism for IBC referrals, not to enable sweeping regulatory directions with systemic effect *sans* government oversight.

By calling Section 35AA an *in personam* power, the Supreme Court essentially said that the RBI cannot issue a one-size-fits-all order that drags every big defaulter into insolvency all at once. This distinction matters because the February 12 circular did exactly that: it gave banks just 180 days to work out a resolution plan for any loan account above INR 2,000 crore, failing which they were forced to start insolvency proceedings under the IBC. In other words, what was meant to solve the NPA problem could have made it worse, turning a slow-moving credit problem into a full-blown systemic crisis.

The Court's insistence that each insolvency reference must be authorised for a specific borrower and default prevents this chain reaction. It forces a more careful, case-by-case approach, giving regulators and lenders time to think about which accounts truly need to go into IBC and which ones can still be rescued through restructuring. This is crucial in a

bank-centric economy like India's, where a shock to bank balance sheets can quickly spread to NBFCs, mutual funds and even healthy companies that rely on bank credit. This is precisely where safe harbour frameworks become relevant. Globally, safe harbours for financial contracts are designed to prevent chain reactions by letting counterparties quickly net exposures and enforce collateral, thus containing the damage to a single, crystallised number rather than leaving it to grow unchecked. Dharani Sugars can therefore be seen as the Indian judiciary's first major step toward recognising the importance of calibration in insolvency policy.

V. EMBEDDING NETTING CERTAINTY AND CALIBRATED SUSPENSION IN INDIA'S BANK-RESOLUTION STATUTE

The design of a bank-resolution statute must be unabashedly practical: its purpose is not to theorise at the level of principle but to manage distress in a way that preserves value. That simple objective, however, sits uneasily between two powerful imperatives. On the one hand, modern markets depend upon predictable private-law mechanics, close-out netting, set-off, and title-transfer collateral, without which intermediation and liquidity collapse. On the other hand, resolution authorities must have the legal space to act fast and decisively when disorder looms. A statute that privileges one objective to the exclusion of the other becomes its own pathology: either it incubates fragility by immunising harmful practices, or it creates paralysis by freezing the plumbing on which recovery depends. The statute must therefore weld safe-harbour into the fabric of resolution law while simultaneously calibrating a narrow, procedural stay that exists

only to permit orderly action and not to become a weapon of indefinite suspension.

At the statute's core should lie a default rule of recognition for the contractual mechanics that constitute market plumbing. Netting and close-out compress exposures make counterparty risk intelligible. They are not incidental conveniences but the scaffolding that allows money markets, derivatives, and repo to function. Where legislatures have conferred immunities, they do so precisely to sustain that plumbing. India's bilateral netting framework supplies important private-law certainty,[41] therefore, a dedicated resolution statute must incorporate and cross-reference that regime so that contractual expectations and statutory emergency powers do not clash. To leave the Netting Act disconnected from the resolution playbook invites litigation and valuation disputes which law is meant to avoid. Recognition of netting is thus a matter of statutory architecture: it converts a fragile assumption into a settled public-law rule that supports contemporaneous resolution planning.

Yet recognition cannot be absolute. Market history demonstrates that the immediacy which makes netting valuable can, in certain markets, most noticeably the repo market, produce catastrophic asset-value contagion when mass liquidations are automatic. It explains how margin calls, rehypothecation, and immediate collateral sales may cause fire sales and systemic spillovers, and it reframes the problem by focusing regulatory attention where contagion actually originates: in assets and liabilities whose

[41] Bilateral Netting of Qualified Financial Contracts Act, 2020, No. 30, Acts of Parliament, 2020 (India).

liquidation can jeopardize markets. The statutory response must therefore be twofold: preserve, prima facie, the enforcement of high-quality QFCs that sustain settlement, and, for instruments whose immediate liquidation would produce contagion, provide a conditional mechanism that temporarily suspends destructive immediacy while triggering a controlled resolution device. That device should supply calibrated liquidity, conservative haircuts, and a managed liquidation timetable so that preservation of value, not wholesale price discovery by panic, governs outcomes.[42]

The practical operation of a conditional suspension must be tightly circumscribed. The RBI Working Group's recommendations offer an administrable template: permit a very short statutory stay, that is sufficient to carry out valuation, effect transfer, or create a bridge transaction, and limit extensions to a single, documented interval for demonstrably necessary reasons. Embedding a forty-eight-hour baseline and a narrowly framed extension in statutory text has two salutary effects. *First*, it supplies the resolution authority with a predictable breathing space to execute a permissible remedy. *Second*, it constrains discretion and reduces the uncertainty that gives rise to opportunistic runs and litigation. The statute should also specify the permitted purposes of the stay and require contemporaneous reasoned orders and ex post accountability such that

[42] Viral V. Acharya & T. Sabri Öncü, *A Proposal for the Resolution of Systemically Important Assets and Liabilities: The Case of the Repo Market*, 9 INT'L J. CENT. BANKING (SYMPOSIUM) 197 (2013).

remedies for improper exercise focus on compensation rather than on disruptive reversals of market-settled transactions.[43]

A tiered approach, which affords unqualified safe harbour to core, high-quality qualified financial contracts, while subjecting Systemically Important Assets and Liabilities ("**SIAL**")-type exposures to a conditional suspension and specialised resolution mechanism, reconciles the competing demands of certainty and systemic protection. For core QFCs, the statute should make prima facie recognition the default, subject only to the brief statutory pause. For SIALs, the statute should authorise a repo-style resolution facility: predefined eligibility for collateral, ex-ante fees, conservative immediate payments calibrated by haircut, and an institutional backstop to manage liquidation risk. This calibrated architecture reduces moral hazard by imposing ex-ante participation conditions while avoiding the self-fulfilling collapse that follows indiscriminate immunities.[44]

Procedural scaffolding is the instrument that converts good policy into practicable law. The statute should require recovery and resolution plans that identify critical contracts and treatment options, a registry or notification mechanism for qualifying contracts, and mandated written findings when the stay is invoked. Judicial or administrative review must be swift, focused, and structured so that remedies preserve the operational continuity of markets. Clawback powers should be narrowly drawn: routine margining and bona fide transfers must be protected to preserve liquidity,

---

[43] Reserve Bank of India, *Report of the Working Group on Resolution Regime for Financial Institutions: Report* (2014) at chs.4-7.

[44] Rizwaan J. Mokal, *Liquidity, Systemic Risk, and the Bankruptcy Treatment of Financial Contracts*, 10 BROOK. J. CORP. FIN. & COM. L. 15 (2015).

while tightly specified avoidance remedies, on grounds of fraud, sham, or deliberate value-stripping within a clear look-back window should remain available to deter and remedy abuse. This procedural package disciplines the exercise of emergency powers without denying the authority the tools it needs to act.

Finally, the statute must be international in orientation. Domestic safe harbour and stays will be of limited efficacy if foreign proceedings routinely negate transfers or close-out determinations. The resolution authority should be empowered to enter into crisis management groups, to share confidential information, and to negotiate recognition protocols with foreign counterparts so that cross-border fragmentation of claims does not convert a local failure into global instability. The combined lessons of the SIAL proposal and the RBI Working Group point to a statute that is simultaneously domestic in force and outward in reach.

If the law is to do what it promises, it must be drafted in the spirit of a traffic manager rather than a barricade. Hence, codify safe harbour where it preserves market functioning, confine the regulatory stay to a short, reasoned, and reviewable pause, tier treatment by contagion risk, protect ordinary market mechanics while retaining narrow, high-threshold clawback powers, and enable cross-border cooperation. Such a synthesis protects value, enables decisive public action, and limits the litigation and paralysis that follow from poorly calibrated emergency powers. The task of statutory drafting is therefore not merely technical, but it is the deliberate

shaping of incentives so that law becomes the instrument that arrests failure without itself becoming a source of value destruction.

VI. CONCLUSION

Whether India requires a bank-specific, sector-specific insolvency playbook that incorporates safe harbours and calibrated resolution mechanisms was the goal of this work. As previously discussed, banks are not just regular debtors; rather, they are systemically important nodes whose failure can trigger collateral fire sales, liquidity freezes, and general credit disruption. In order to prevent contagion without freezing the market's plumbing, jurisdictions like the US and the EU have already incorporated safe-harbour protections into their bank-resolution regimes, according to our analysis of international practice. These jurisdictions carefully balance contractual certainty with limited resolution stays. In comparison, India's stance is still divided. Although the recognition of close-out netting rights by the Netting Act has given a foundation, it functions independently and outside of a framework for comprehensive settlement. The Supreme Court's recognition of the perils of universally applicable insolvency triggers is reflected in judicial rulings like Dharani Sugars. However, the lack of a statutory bank-resolution mechanism still leaves the system dependent on ad hoc, regulator-driven rescues, like those that occurred in the Yes Bank and PMC Bank crises. Although they give short-term stability, these interventions lack the precise sequencing and predictability that a dedicated statute may provide.

Due to the dearth of existing discussion on the subject matter, the article builds its content by way of analogy and discussions from the securities market sector. Nevertheless, the way forward must therefore be holistic. A robust bank-resolution framework must weld safe-harbour protections into its core, ensuring that contractual termination, netting, and collateral enforcement rights remain reliable even during resolution, subject only to a narrowly defined, time-bound stay. In order to guarantee that contractual termination, netting, and collateral enforcement rights are dependable even during resolution, subject only to a strictly specified, time-bound stay, a strong bank-resolution framework must incorporate safe-harbour protections into its very foundation.

By separating riskier assets and avoiding the transfer of failing portions of a bank's balance sheet to its core deposit and payment operations, bankruptcy-remote SPVs can be used to supplement this structure. Critical market infrastructure can be protected by well-designed SPVs, which also free up resolution authorities to concentrate on the problematic aspects of the organization without immobilizing the entire system. The ultimate objective is to make bank failures manageable rather than to protect them from failure. A calibrated combination of safe harbours, resolution choreography, and bankruptcy-remote structuring would convert what is today a largely reactive, discretionary process into a predictable, rule-based regime. Such a regime would compress exposures quickly, prevent fire-sale contagion, and give regulators the breathing space to orchestrate orderly resolutions preserving both systemic stability and

creditor confidence. For a bank-centric economy like India's, this is not merely desirable; it is essential to ensure that the next major bank failure does not metastasize into a full-blown financial crisis