
BEYOND GREEN MASKS: TECHNOLOGY, CRIMINAL LIABILITY, AND THE BATTLE AGAINST ESG FRAUD IN THE NEW ECONOMY

Aakanksha Verma, Institute of Law, Nirma University

ABSTRACT

When it comes to environmental, social, and governance investing, this has moved from a marginal part of responsible finance to the heart of it, totally changing the way trillions of dollars are deployed and the way regulating bodies gauge the responsibility of corporations. It has produced one of the most sophisticated and under-prosecuted forms of corporate misconduct in the new economy: ESG fraud. This essay examines a specific and underappreciated dimension of that problem. The central research question is not merely whether companies misrepresent sustainability claims, but whether the legal frameworks designed to hold them accountable have kept pace with the technology through which those misrepresentations are now engineered.

The scope of analysis covers three interconnected domains. First, it examines the technological paradox at ESG's core: the same tools promoted as instruments of accountability, algorithmic reporting, blockchain supply chains, and AI-generated disclosures have become the primary mechanisms of concealment. Second, it diagnoses how that technological reality has broken three foundational doctrines of corporate criminal liability: the identification doctrine's requirement of a directing mind, veil-piercing's assumption of traceable control, and materiality standards premised on conscious human intent. Third, it provides a comparison of regulatory reactions in India, the European Union, and the United States, and it proves that all the frameworks address the problem they were aimed at, only as a part of it.

The essay is organized in six sections, which are diagnosing the technology paradox, mapping doctrinal failure in terms of identification, veil-piercing, and materiality, comparing regulatory frameworks, analyzing governance as the location linking failure to fraud, proposing technology-based enforcement tools, and providing legislative, regulatory, and governance recommendations. The core argument is that closing the accountability gap requires doctrinal reconstruction. Anything less leaves ESG as what it has already too often become, a sophisticated instrument for manufacturing plausible deniability at an industrial scale.

INTRODUCTION

In May 2022, the raiding of the Frankfurt offices of DWS Group, an asset management unit of Deutsche Bank, was carried out on the basis of incriminating claims put forward by a former sustainability chief of the company, Desiree Fixler. Such was not a problem of excessive marketing or inaccurate bookkeeping as Fixler described. It was far more prone to calculation: the company had massively exaggerated the degree to which the ESG standards had any impact on its investment policy, and the investors who thought they were investing in sustainable finance were left with a slick fiction. As of 2023, the SEC had fined the company up to 25 million dollars, and in 2025, the German prosecutors affirmed a fine of another 25 million dollars for negligent misrepresentation.¹

The DWS scandal is worth commenting on, not merely as a moral lesson on business malpractice. What renders it truly educative is what it indicates under the hood, a contradiction that is installed at the core of ESG in the new economy. Algorithms, blockchain-based tracking of supply chains, AI-generated disclosures, and so on, the technologies that were claimed to render sustainability claims auditable and honest have, in practice, provided a more advanced repertoire to bad actors to make and hide disclosures.² The transparency promise turned out to be an anti-transparency veil. It is not an incidental phenomenon. And it demands a structural response.

This essay advances an underexplored argument: technology has not merely enabled ESG fraud, it has fundamentally broken the doctrinal assumptions on which corporate criminal liability rests. The identification doctrine presumes a “directing mind.” Algorithmic misconduct has none. Veil-piercing presumes identifiable control. Automated systems obscure it. Materiality standards presume human intent. The artificial intelligence systems that are trained with false data will generate fraud, even though it is not the intention of anyone to do so. To end the accountability gap, it is necessary to reconstruct the liability doctrine based on these realities, rather than simply add tech-enforcement devices to the existing systems. Without such reconstruction, ESG risks will become the most sophisticated vehicle for white-collar crime the new economy has produced.

¹ Press Release, U.S. Sec. & Exch. Comm’n, SEC Charges DWS Investment Management Americas for ESG Misstatements (Sept. 1, 2023), <https://www.sec.gov/news/press-release/2023-159>.

² John C. Coffee Jr., *Corporate Crime and Punishment: The Crisis of Underenforcement* 6–18 (Berrett-Koehler Publishers 2020).

THE TECHNOLOGY PARADOX AT THE HEART OF ESG FRAUD

Partly due to a promise of technology, ESG disclosure became possible: the use of digital tracking, satellite imagery, and AI-generated reports would for the first time enable the scaling up of corporate sustainability claims. That's a promise that's been turned upside down. Nowadays, the same instruments are used to deceive.

This paradox is best exemplified in blockchain. It's touted as a solution to transparency in the supply chain, but for those who promote its use, it's a principle that is seldom highlighted: garbage in, garbage out. Businesses develop complex digital footprints to seemingly verify ethical sourcing. The immutable record looks authoritative. But if original data entries are false, claiming conflict-free minerals from war zones, certifying organic cotton that is conventionally grown, the blockchain does not detect the lie. It preserves and legitimizes it. Immutability, the technology's defining virtue, becomes its defining vulnerability: a fraudster embeds the lie once, and it cannot be corrected.³

Critically, though, this is a different problem from what AI reporting systems create. Blockchain's vulnerability is conventional data fraud that the technology merely preserves; the wrong is committed upstream, before the digital record is made. Algorithmic ESG reporting presents a genuinely distinct and more dangerous risk: the system itself is engineered to produce misleading outputs. Parameters can be calibrated to favor certain metrics while downplaying others. The approach to carbon accounting can be applied selectively, taking Scope 1 and Scope 2-based emissions data when convenient, and no Scope 3 supply chain data when this data often makes up most of the environmental impact.⁴ More insidiously still, the machine learning model can be trained on a set of data that is intentionally skewed, giving the impression of being technically right within its intended scope, yet misleading on scales of operation. This is not hypocrisy; it is structural fraud, which is facilitated by technological complexity, and that must be addressed as such. Complexity of the mechanism does not reduce culpability.⁵ It intensifies it, which shows premeditation.

³ Kevin Werbach, *The Blockchain and the New Architecture of Trust* 135–151 (MIT Press 2018).

⁴ Katharina Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* 89–112 (Princeton Univ. Press 2019); Roberto Palea & Lara Drogo, Carbon Emissions and Financial Performance: The Moderating Role of ESG Ratings, 31 *Bus. Strategy & Env't* 3138, 3140 (Dec. 2022).

⁵ Cary Coglianese & Alicia Lai, Algorithmic Regulation and ESG Governance, 71 *Duke L.J.* 191, 218–227 (2021).

These processes are manifested in the fashion industry. In 2023, H&M settled on false sustainability scorecards that had introduced algorithmically arranged measures without specifying that they selected these measures in the first place,⁶ and investigations by independent researchers found toxic dyes, textile theft, and tons of textile waste at supplier plants are concealed behind layers of subcontractors. Technology presents something that makes it seem transparent to the extent of actively precluding examination.⁷

Since ESG metrics started determining credit ratings, stock prices, and access to capital, what used to be a voluntary undertaking turned into a financial matter of substance.⁸ Technology changed that even more. It has become automatic that capital flows based on ESG scores are influenced by algorithmic portfolio screening by institutional investors. Companies that have perfected algorithmic self-presentation, i.e., achieving high points in machine-readable indicators despite the state of affairs in their activities, raise billions of dollars in investments, which financially responsible businesses are unable to find. Technology designed to reward sustainability rewards its simulation instead.⁹

Civil penalties have proven an inadequate response. A \$25 million fine for a multi-billion dollar asset manager is a rounding error, a predictable cost of doing business.¹⁰ Criminal liability carries something civil penalties cannot: the condemnatory weight of society's strongest judgment. Possible jail time for the executives, a ban on government contracts, a long-term reputational impact, all these change the calculations in a way that fines will never.¹¹

DOCTRINAL BREAKDOWN: HOW TECHNOLOGY DEFEATS EXISTING LIABILITY FRAMEWORKS

A. The Algorithmic Blind Spot of the Identification Doctrine.

The traditional concern of corporate criminal liability was that a corporation has no

⁶ Norwegian Consumer Authority, *Assessment of H&M's Sustainability Claims* (2023); European Consumer Organisation (BEUC), *Greenwashing: How to Stop Companies from Misleading Consumers* 8–12 (2022).

⁷ Changing Markets Found., *Synthetics Anonymous: Fashion Brands' Addiction to Fossil Fuels* 12–28 (2021); Elizabeth L. Cline, *The Conscious Closet* 45–67 (Plume 2019).

⁸ Principles for Responsible Inv., *PRI: An Introduction to Responsible Investment* (2022), <https://www.unpri.org>.

⁹ OECD, *ESG Investing: Practices, Progress and Challenges* 17–29 (2020).

¹⁰ Brandon L. Garrett, *Too Big to Jail: How Prosecutors Compromise with Corporations* 234–256 (Belknap Press 2014).

¹¹ Henry M. Hart, Jr., *The Aims of the Criminal Law*, 23 *Law & Contemp. Probs.* 401, 404–06 (1958).

physical presence or consciousness;¹² criminal law requires the state of being guilty (*actus reus*) and guilty (*mens rea*), which is a problem because no one can find criminal intent in the corporation itself.¹³ This issue was addressed by the identification doctrine, which held that criminal intent is present in the directing mind and will of the corporation whose decisions could be attributed to the corporation.¹⁴

This scheme is broken by algorithmic ESG fraud. When a machine learning model is trained on a dataset engineered to produce misleading outputs, no single executive “decides” to deceive. The decision is distributed across dozens of technical choices: which variables to include, which methodologies to weight, which validation benchmarks to apply. A sustainability officer who approves a report generated by such a system may genuinely believe its outputs are accurate. The deception is embedded in system architecture, not in any identifiable individual’s conscious choice.¹⁵ The directing mind is nowhere. The fraud is everywhere.

The self-evidently opposing doctrine is the doctrine of willful blindness, which the courts of the U.S. have resorted to when implementing it when the defendants knowingly and voluntarily remain ignorant of the misconduct in their own systems.¹⁶ This is the most natural doctrine answer, and it is applicable to cases, namely, of executives who knowingly and voluntarily remain unaware of the misconduct in their own systems. Still, willful blindness must be proven by intentional neglect, and it is still based on personal cognition. It does not address institutional configurations where nobody had reason to ask the question in the first place, because the incentive structures rewarding misleading outputs were themselves the fraud. When an executive compensation committee ties sustainability bonuses to ESG score improvements and a data team adjusts algorithmic parameters accordingly, no one needs to avoid knowing anything. The system’s incentive structure delivers the deception automatically.

U.S. law’s broader vicarious liability standard, holding corporations liable for any

¹² Gerhard O.W. Mueller, *Mens Rea and Corporate Criminal Liability*, 19 U. Pitt. L. Rev. 21, 23–34 (1957).

¹³ V.S. Khanna, *Corporate Criminal Liability: What Purpose Does It Serve?*, 109 Harv. L. Rev. 1477 (1996).

¹⁴ *Tesco Supermarkets Ltd v. Nattrass* [1972] A.C. 153 (H.L.) (U.K.); *Lennard’s Carrying Co. v. Asiatic Petroleum Co.* [1915] A.C. 705 (H.L.) (U.K.).

¹⁵ Woodrow Barfield & Ugo Pagallo, *Advanced Introduction to Law and Artificial Intelligence* 95–108 (Edward Elgar Publishing 2020).

¹⁶ *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769 (2011) (holding willful blindness requires subjective belief in high probability and deliberate avoidance of truth); *United States v. Jewell*, 532 F.2d 697 (9th Cir. 1976) (en banc) (applying conscious avoidance doctrine to criminal knowledge).

employee's acts within employment scope, reaches further but still misses the deeper problem.¹⁷ When wrongdoing is systemic, embedded in algorithmic design, encouraged by incentive structures that reward favorable metric performance, facilitated by deliberate gaps in oversight, pinning liability on individual actors misses the forest for the trees. The crime is the corporation's operational model. Liability doctrine must say so explicitly.¹⁸

Product liability law offers the sharpest analogy. It long struggled with the same question when manufacturing defects caused harm without any individual worker consciously producing a faulty unit. The answer was strict liability attaching to the manufacturer regardless of individual fault, because the manufacturer controlled the system that produced the defect, and the harm was foreseeable.¹⁹ Applied to ESG fraud, the analogy runs as follows: when a corporation deploys an algorithmic reporting system, and that system predictably generates misleading sustainability metrics, the corporation is the manufacturer of the deception even if no single employee intended it. But the analogy requires careful specification. The best comparison is design defect liability, rather than manufacturing defect: the claim is not that a normally functioning system happened to generate an aberrant output, but that the system was designed in a manner that generated misleading output, which was its normal and foreseeable effect. Under this framing, the causation analysis is direct, the biased parameter choices are the proximate cause of the false disclosures, and the company that commissioned the system design is the liable party. The distributed nature of the harmful act across machine and human decisions does not dissolve corporate culpability; it relocates it from the individual to the institution. Legislatures that have accepted strict corporate liability in product safety contexts have no principled reason to resist its application here.

B. Piercing the Veil When Technology Obscures Control

Veil-piercing, holding parent companies liable for subsidiary misconduct, becomes both more necessary and more technically difficult in the digital economy.²⁰ Environmental

¹⁷ United States v. Hilton Hotels Corp., 467 F.2d 1000, 1004 (9th Cir. 1972); U.S. Dep't of Justice, *Principles of Federal Prosecution of Business Organizations* § 9-28.500 (2015).

¹⁸ Pamela H. Bucy, Corporate Criminal Liability: When Does It Make Sense?, 46 Am. Crim. L. Rev. 1437, 1445–1468 (2009).

¹⁹ Restatement (Third) of Torts: Prods. Liab. § 2 (Am. Law Inst. 1998); see also Greenman v. Yuba Power Prods., Inc., 59 Cal. 2d 57, 62 (1963).

²⁰ Robert B. Thompson, Piercing the Corporate Veil: An Empirical Study, 76 Cornell L. Rev. 1036, 1038–42 (1991).

and social harms are routinely conducted through thinly capitalized subsidiaries designed to absorb liability while parent corporations reap profits.²¹ When disaster strikes, the shell entity dissolves, leaving communities to bear the damage.²²

UK courts have moved in the right direction. In *Vedanta Resources Plc v. Lungowe*, the Supreme Court held that parent companies could owe direct duties of care when they exercised significant control over relevant subsidiary policies.²³ *Okpabi v. Royal Dutch Shell* extended this reasoning: multinationals that set group-wide strategic direction and establish shared technical systems cannot credibly claim ignorance of subsidiary operations.²⁴ These precedents need extending into ESG fraud specifically. When a parent company deploys group-wide ESG reporting software, sets the parameters by which subsidiaries' sustainability data is collected and aggregated, and then markets consolidated ESG metrics to investors, control over the disclosure system is undeniable regardless of formal corporate separateness. Consolidated sustainability reporting implies consolidated liability when those metrics prove fraudulent.

C. Materiality and Algorithmic Intent: Updating the Probability-Magnitude Test

The probability-magnitude test from *Basic Inc. v. Levinson* assesses materiality by weighing the likelihood of an event against the significance of its impact.²⁵ The framework requires modification applied to algorithmic ESG fraud. The issue of probability should go further than whether or not a misstatement could be identified to whether or not system designers were aware or ought to have been aware that their algorithmic decisions would systematically generate false results.

To make the practical difference concrete, consider how DWS's reporting algorithms would be analyzed under the existing test versus the proposed extension. Under the existing test, a court asks whether each disclosed metric was likely to be detected as false and, if so, whether it was significant enough to affect investment decisions. The architects of DWS's reporting system made choices about which data sources to include, which

²¹ Phillip I. Blumberg, Limited Liability and Corporate Groups, 11 J. Corp. L. 573, 580–605 (1986).

²² Peter Muchlinski, Implementing the New UN Corporate Human Rights Framework, 22 Bus. Ethics Q. 145, 158–65 (2012).

²³ *Vedanta Res. Plc v. Lungowe* [2019] UKSC 20 (U.K.).

²⁴ *Okpabi v. Royal Dutch Shell Plc* [2021] UKSC 3 (U.K.).

²⁵ *Basic Inc. v. Levinson*, 485 U.S. 224, 238–39 (1988).

methodologies to weight, and how to handle outliers that predictably produced favorable outputs, but that inquiry gets lost because no single disclosure decision is traced back to an identifiable deceptive choice.²⁶ Under the extended test, the relevant probability is not merely the odds of detection: it includes the foreseeable likelihood that biased system design would produce misleading outputs in the first place. The magnitude analysis then captures not just one disclosure but the systematic misallocation of billions in capital. The designers of a reporting system that is foreseeably biased towards its results ought to be exposed to the same materiality discovery as an individual who lies about one number; the deliberate act to so lie is inherent in the design, and not the results.

COMPARATIVE FRAMEWORKS: DIVERGENT RESPONSES TO A SHARED CHALLENGE

A. India: Disclosure Without Verification Architecture

India's Business Responsibility and Sustainability Report (BRSR), mandated by SEBI for the top 1,000 listed companies, represents a genuine transparency advance.²⁷ Its fatal structural weakness is that assurance remains voluntary. Companies issue assertions; no one is methodically held to ascertain them.²⁸ Laws are enforced in a disjointed way between the Ministry of Corporate Affairs and SEBI and between environmental agencies, creating a jurisdictional overlap that is being taken advantage of by complex players.²⁹ Research that develops greenwashing scores of Indian companies by comparing BRSR claims and the actual performance indicators shows that there is systematic overstatement, especially on emissions mitigation and CSR spending.³⁰

What this literature demonstrates is not simply that companies lie. It is that the BRSR framework creates no technological architecture for catching lies, no satellite verification, no algorithmic cross-referencing, and no AI-powered anomaly detection. The BRSR is a disclosure regime without a verification regime. In the new economy, that gap is not a

²⁶ Donald C. Langevoort, Disclosures That "Bespeak Caution," 49 Bus. Law. 481, 487–502 (1994).

²⁷ Sec. & Exch. Bd. of India, Business Responsibility and Sustainability Report, Circular No. SEBI/HO/CFD/CMD2/P/CIR/2021/562 (May 10, 2021).

²⁸ Ministry of Corporate Affairs (India), National Guidelines on Responsible Business Conduct (2019).

²⁹ Afra Afsharipour, Corporate Law in the Age of Sustainability Reporting, Ohio St. Bus. L.J. 1, 28–35 (2022).

³⁰ Pawan Kumar Vijay & Rajesh Sharma, Greenwashing: A Study of Indian Companies, J. Corp. Governance, Mar. 2023, at 67, 72–89.

design flaw. It is an invitation.

India also faces concentrated ownership challenges. Founding families and promoter groups controlling major enterprises limit independent oversight and make challenging questionable algorithmic reporting practices institutionally difficult.³¹ The SEC has demonstrated that governance quality and disclosure quality are inseparable. Investigations scrutinize not just whether claims were false but what systems produced them and who oversaw those systems. India's enforcement approach has yet to internalize this lesson.³²

B. The EU and United States: Ambitious Frameworks, Persistent Gaps

The Corporate Sustainability Reporting Directive of the EU will incorporate detailed and audited reporting in line with the European Sustainability Reporting Standards, compared to the scheduled Corporate Sustainability Due Diligence Directive, which will require an impact evaluation of the value chain and civil liability in the event of failures.³³ These frameworks are the most ambitious globally. Their shared limitation is the same one that plagues every disclosure-based approach: mandatory auditing addresses the accuracy of reported data but does not reach the design of the reporting systems that generate it. An auditor can verify that a company reported what its algorithm produced. The auditor cannot easily determine whether the algorithm was constructed to produce misleading results.³⁴

The United States has moved most aggressively in securities fraud enforcement. The SEC's Climate and ESG Task Force applies established materiality, scienter, and damages precedents to sustainability misrepresentations, treating false ESG claims affecting investment decisions as securities fraud.³⁵ The DWS settlement, combining civil penalties with a Department of Justice criminal investigation, demonstrates the coordinated approach's potential. Yet even this approach predominantly protects investors rather than environmental and social harm victims, and it does not systematically address

³¹ Umakanth Varottil, *Evolution and Effectiveness of Independent Directors in Indian Corporate Governance*, 9 *Hastings Bus. L.J.* 281, 298–315 (2015).

³² Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges Goldman Sachs Asset Management for ESG Disclosure Failures, Press Release No. 2022-120 (June 22, 2022).

³³ Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 Amending the Corporate Sustainability Reporting Directive, 2022 O.J. (L 322) 15; Proposal for a Directive on Corporate Sustainability Due Diligence, COM (2022) 71 final (Feb. 23, 2022).

³⁴ Beate Sjøfjæll, *Sustainable Value Creation Within Planetary Boundaries*, *Sustainability*, Apr. 2020, at 1, 1–19.

³⁵ Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Enforcement Task Force Focused on Climate and ESG Issues (Mar. 4, 2021), <https://www.sec.gov/news/press-release/2021-42>.

algorithmically embedded misrepresentation.

Comparing these frameworks honestly, each captures a piece of the problem. India discloses without verifying. The EU audits outputs without examining the systems generating them. The U.S. applies securities doctrine effectively but has not fully confronted algorithmic mens rea. None has achieved the comprehensive reconstruction this problem demands.

C. Technology-Accelerated Regulatory Arbitrage

These conflicting systems pose regulatory arbitrage opportunities, which technology has rendered exceedingly simpler to leverage. Digital operations can be relocated instantly; intellectual property licensed across borders shifts profits; data centers positioned strategically claim favorable jurisdictional treatment.³⁶ The physical world's friction, which historically constrained how quickly companies could restructure to evade accountability, has largely evaporated. International cooperation remains critically underdeveloped. Enforcement is fundamentally national, while corporations operate globally in real time. Mutual legal assistance treaties move at a diplomatic pace; corporations move at an algorithmic pace. The imbalance is not by chance.

GOVERNANCE AS THE HUMAN CONTROL LAYER, AND AS A DOCTRINAL CATEGORY

The comparative analysis shows one pattern, all frameworks that do not propose solutions to address algorithmic ESG fraud fail the governance layer first. Governance is not a separate topic. It is the mechanism through which doctrinal failures and technological complexity combine to produce fraud,³⁷ and it is therefore the site at which legal intervention would be most directly effective.

In the algorithmic age, governance means something more specific than independent boards and transparent auditing. It involves having human control over automated systems, which would have been optimized to perform metrics instead of being truly sustainable. The prevalent failures of governance allow ESG fraud to occur in a multiplicative manner with

³⁶ See Jennifer Zerk, *Multinationals and Corporate Social Responsibility* 78–104 (Cambridge Univ. Press 2006).

³⁷ OECD, *Corporate Governance and ESG Integration* 11–25 (2021).

technological complexity: boards that lack truly independent status with the management, compensation systems that give bonuses based on positive ESG ratings, audit committees that are not also technologically sophisticated to analyze algorithmic reporting systems, and compliance functions that should be checking the activities of the executives they are assessing.³⁸

How the governance failure is converted into the algorithmic fraud is a mechanism that is worth following. Consider a plausible sequence: an executive compensation committee ties sustainability bonuses to ESG score improvements. A data team, facing that incentive, adjusts the parameters of the Scope 3 emissions calculation to exclude upstream supplier categories. A sustainability officer signs off on the resulting report without querying the methodology change. A board audit committee reviews aggregate figures but lacks the technical literacy to recognize that the underlying model has been quietly rewritten. At no point does anyone issue an instruction to lie. Yet the output is false. And under the current doctrine, nobody is clearly criminally liable.

This is why governance failures should be treated as doctrinal failures of the third kind, after the identification doctrine's blind spot and veil-piercing's inadequacy. Legal reform that imposes liability on firms that cannot demonstrate genuine algorithmic oversight is not an overreach. It is recognition of how corporate deception actually works. This connection has been made explicit by the SEC, in which the examination is not whether certain disclosures were false so much as it is how governance systems generated them: who looked at the data, what power had the board over the design of algorithms, whether they were internal warnings of wrongful actions or systemic indifference.³⁹

TECHNOLOGY AS SOLUTION: REBUILDING ENFORCEMENT FROM THE GROUND UP

If technology has broken existing liability frameworks, it must also rebuild enforcement. Natural language processing can scan corporate disclosures for inconsistencies between formal filings and public communications.⁴⁰ When executives privately discuss metrics

³⁸ Lucian A. Bebchuk & Roberto Tallarita, *The Illusory Promise of Stakeholder Governance*, 106 *Cornell L. Rev.* 91, 128–45 (2020); Donald C. Langevoort, *Cultures of Compliance*, 54 *Am. Crim. L. Rev.* 933, 945–52 (2017).

³⁹ SEC Charges Goldman Sachs Asset Management for ESG Disclosure Failures, *supra* note 22.

⁴⁰ Harry Surden, *Machine Learning and Law*, 89 *Wash. L. Rev.* 87, 115–34 (2014).

diverging from reported figures, AI processing of internal communications can surface evidence of knowing misrepresentation buried in millions of emails, directly addressing the identification doctrine's gap, since even where no individual "decided" to deceive, internal communications may reveal collective awareness of misleading outputs.

Remote sensing and satellite imagery provide an independent verification system that circumvents the corporate reporting system altogether. When a company boasts of reforestation, but satellite images indicate that they continue to deforest, no manipulation of some parameter of the algorithm can mask the physical fact. This is what the blockchain paradox requires: not to trust the digital trail, but to establish the facts underlying it oneself.⁴¹

Sensors at the production sites can deliver real-time monitoring of emissions, which will exclude the use of self-reported data. Water quality sensors can detect the discharge of pollutants in real-time; air quality monitors will measure the emission of particulate matter; energy consumption sensors will enable facilities to use a renewable power source or only purchase carbon credits. These sensors, once prohibitively expensive, have reached price points permitting widespread regulatory deployment. Financial transaction monitoring addresses the veil-piercing challenge, machine learning excels at identifying suspicious fund flows, circular transactions through related entities, and green investment capital funding conventional projects.⁴²

Predictive analytics will be able to facilitate proactive enforcement as opposed to reactive. Through disclosure language analysis, the structure and scale of the governance, executive compensation incentives, and peer-industry comparisons, algorithms are capable of generating risk scores that signal enterprises that should be investigated before the mitigation of fraud has reached its ultimate consequences. The U.S. Department of Justice already employs such analytics for corporate compliance monitoring.⁴³

⁴¹ David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. Davis L. Rev. 653, 682–97 (2017).

⁴² Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 Berkeley Tech. L.J. 487, 512–29 (2018).

⁴³ U.S. Dep't of Justice, *Evaluation of Corporate Compliance Programs* 14–17 (updated June 2020).

RECOMMENDATIONS: REBUILDING LIABILITY FOR THE ALGORITHMIC AGE

A. Legal Reforms: Doctrinal Reconstruction

India's Companies Act, 2013, and SEBI regulations should be amended to explicitly criminalize knowing or reckless ESG misrepresentation, with penalties scaling to harm magnitude, significant corporate fines, potential imprisonment for responsible officers, and debarment for repeat offenders.⁴⁴ A "failure to prevent greenwashing" provision modeled on section 7 of the UK Bribery Act would impose strict liability on corporations absent adequate compliance systems, including adequate oversight of ESG reporting algorithms. The parallel to the Bribery Act is deliberately chosen: that provision has transformed UK corporate compliance culture not by generating convictions but by forcing companies to implement genuine preventive systems to establish adequate procedures for defense. The same incentive structure is precisely what ESG fraud enforcement needs to create.⁴⁵

The identification doctrine requires explicit legislative updating.⁴⁶ Courts should be directed to find corporate mens rea where algorithmic systems were designed with knowledge that they would predictably produce misleading outputs, whether or not any individual consciously chose to deceive. The probable objection is that this standard is too open-ended, capturing good-faith algorithmic error alongside deliberate fraud. The response is that existing law already handles this distinction: the standard requires knowledge of predictable misleading outputs, not merely knowledge that algorithmic design involves choices. A company that commissions system design, receives internal warnings that outputs are skewed, and continues deployment without correction has demonstrated the requisite knowledge. One that deploys a system without any review mechanism has demonstrated the willful blindness that existing doctrine already penalizes. Neither formulation sweeps in genuine error.

The probability-magnitude materiality test should be codified with explicit extension to biased system architecture as described in Section II.C, and courts should be empowered to pierce the corporate veil wherever parent companies deploy shared algorithmic ESG

⁴⁴ Bribery Act 2010, c. 23, § 7 (U.K.); Jennifer Arlen, *The Failure of the Organizational Sentencing Guidelines*, 66 U. Miami L. Rev. 321, 334–48 (2012).

⁴⁵ U.K. Ministry of Justice, *The Bribery Act 2010: Guidance* 14–20 (2011).

⁴⁶ Celia Wells, *Corporate Criminal Liability: A Ten-Year Review*, 13 Crim. L.F. 283, 286–305 (2002).

reporting infrastructure across subsidiaries. Consolidated technology implies consolidated accountability.⁴⁷

B. Regulatory Reforms: Verification Architecture

Mandatory third-party assurance for BRSR disclosures by auditors with environmental and social expertise would close India's most glaring gap, but assurance of reported outputs is insufficient without assurance of the systems generating them. Regulators must develop standards for auditing ESG reporting algorithms themselves, examining parameter choices, training datasets, and validation methodologies for evidence of deliberate bias.⁴⁸ Improved whistleblower laws and incentives based on the U.S. False Claims Act would motivate internal disclosure of data scientists and engineers who notice that systems are being tuned to lie.⁴⁹

C. Technological Integration: Capacity of Enforcement.

To reduce the impact of algorithmic architecture, SEBI and environmental regulators are advised to design special technology enforcement units, employing data scientists and engineers familiar with the enforcement priorities as well as the structure of the algorithm. The first priorities must involve automated disclosure scanning to detect statistical indicators of anomalies, satellite-based independent verification of environmental claims, and monitoring of financial transactions to see CSR funds diversion by multinationals.⁵⁰ An international data-sharing agreement would allow international investigation of multinationals making use of jurisdictional arbitrage.

D. Governance Standards and International Harmonization

Board composition should ensure at least one director with demonstrated ESG and technology credentials capable of interrogating algorithmic reporting systems, not merely approving their outputs.⁵¹ Executive compensation clawback provisions should be triggered

⁴⁷ *Basic Inc. v. Levinson*, 485 U.S. 224 (1988); *see supra* Section II.C.

⁴⁸ Jill E. Fisch, *Making Sustainability Disclosure Sustainable*, 109 *Geo. L.J.* 923, 956–71 (2020).

⁴⁹ 31 U.S.C. §§ 3729–3733; David Freeman Engstrom, *Public Regulation of Private Enforcement*, 107 *Nw. U. L. Rev.* 545 (2013).

⁵⁰ Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 *Geo. L.J.* 1147, 1182–1201 (2017).

⁵¹ Lucian Bebchuk, Jesse Fried & David Walker, *Managerial Power and Rent Extraction in the Design of Executive Compensation*, 69 *U. Chi. L. Rev.* 751, 788–802 (2002).

by the discovery of material misrepresentation. Audit committees should have explicit authority to engage independent technical experts to evaluate ESG reporting system design.

Extraterritorial jurisdiction for ESG fraud, modeled on the Foreign Corrupt Practices Act, would allow major capital markets to prosecute companies whose false disclosures affected their investors, regardless of incorporation jurisdiction.⁵² This has to be carefully calibrated, and the regulatory imperialism objection should not be thrown away but rather should be dealt with in full.

It is a valid objection in the case of substantive operational criteria: the fact that a factory in Dhaka has Dutch environmental standards can legitimately question the sovereignty and fairness of development. The jurisdiction suggested here is less broad. It is not the environmental performance of the factory that is being regulated, but the precision of the disclosure that was given to the investors in Frankfurt or Mumbai. The financial regulation precedents are enlightening. The FCPA has been closely operating in the past 50 years without being branded as American regulatory imperialism, as its jurisdictional scope is not based on the enforcement of the U.S. ethical standards but safeguarding the integrity of the capital markets to which the companies have voluntarily become members. A similar principle applies here in that a firm that decides to raise capital in an advanced market internalizes the disclosure rules of the advanced market as a prerequisite to access, just as it internalizes the local contract law and securities regulation when it lists on a foreign exchange. The relevant question is not whether host-country environmental standards were violated but whether investors in the capital-access market were deceived about what those standards were, a question that belongs squarely to the market where the deception occurred. Courts and legislators should say so plainly, preempting the regulatory imperialism argument before it becomes a shield for sophisticated fraud.

International treaties on ESG fraud enforcement, establishing mutual recognition of investigations and coordinated sanctions, would complete the architecture. The Basel Committee and FATF demonstrate that such coordination is achievable when political will and economic alignment exist.⁵³

⁵² 15 U.S.C. § 78dd-1; Mike Koehler, *The Foreign Corrupt Practices Act in the Ultimate Year of Its Decade of Resurgence*, 43 Ind. L. Rev. 389, 402–18 (2010).

⁵³ Basel Comm. on Banking Supervision, *Core Principles for Effective Banking Supervision* (2012); Fin. Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism &*

CONCLUSION

The central problem of ESG enforcement in the new economy is not that regulators lack rules. It is that their rules were designed for a world where fraud required a human being to consciously decide to lie, where corporate control could be traced through organizational charts rather than algorithmic infrastructure, and where the tools of verification and the tools of deception were distinct. Technology has collapsed all three assumptions simultaneously.

This essay has argued for a specific reconstruction. The identification doctrine must be updated to recognize that algorithmically embedded misrepresentation constitutes corporate mens rea, whether or not any individual consciously chose deception. The product liability analogy, specifically, design defect liability, provides the doctrinal mechanism: the corporation that commissions a system designed to produce misleading outputs is the manufacturer of the deception. Veil-piercing doctrine must extend to shared technological infrastructure as a marker of effective control. The probability-magnitude materiality standard must encompass the foreseeable consequences of biased system design. And enforcement must deploy the same technological sophistication as fraud, AI anomaly detection, satellite verification, IoT monitoring, and financial transaction analysis, to close the evidentiary gaps that algorithmic fraud deliberately creates.

The nearest-term legislative target is achievable. A “failure to prevent greenwashing” strict liability provision, modeled on the UK Bribery Act’s section 7, would not require the full doctrinal reconstruction described above; it would simply force companies to implement and document genuine algorithmic oversight systems or face liability when those systems produce misleading results. That single reform, properly implemented, would transform the compliance incentives that currently make algorithmic fraud attractive. It is the right first move.

There is something telling about the specific form ESG fraud takes. It does not announce itself. It does not announce itself. It comes in the language of responsibility, carbon commitments, supply chain audits, board diversity targets, and plants the fraud in the very systems that should confirm such statements. That is a different kind of fraud from a lie. It is fraud that corrupts the infrastructure of accountability itself, making the instruments of trust into

Proliferation (2012), updated 2023.

instruments of concealment. Doctrines built for a world of identifiable human decisions and traceable corporate hierarchies are not equipped to hold algorithmic systems to account. Fixing that requires acknowledging that the most sophisticated bad actors today are not forging documents or bribing auditors; they are engineering the measurement systems themselves. Until the law treats that for what it is, ESG will remain what it has too often been: a beautifully designed instrument for the mass production of plausible deniability.